НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки

Кафедра електронних приладів та пристроїв

«До захисту допущено»
Завідувач кафедри

_____ Л.Д. Писаренко
“___”_____ 2019 р.

Дипломний проект

освітньо-кваліфікаційного рівня «Бакалавр»

з напряму підготовки **6.050802 – Електронні пристрої та системи**

на тему: « Цифровий перетворювач звукових сигналів »

Виконав:
студент 4 курсу, гр. ДЕз-41 **Хорольський Євген Віталійович**_____

Керівник:
доцент кафедри ЕП та П, к.т.н., доц. **Цибульский Л. Ю.**___ _____

Нормоконтроль:
доцент кафедри ЕП та П, к.т.н., доц. **Чадюк В. О.** _____

Рецензент

_____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цьому дипломному проекті немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Київ – 2019

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки
Кафедра електронних приладів та пристроїв

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки (програма професійного спрямування) – 6.050802 –

Електронні пристрої та системи (Електронні прилади та пристрої)

ЗАТВЕРДЖУЮ
Завідувач кафедри, проф., д.т.н.
_____ Л.Д.Писаренко
«____»_____ 2019 р.

ЗАВДАННЯ

на дипломну роботу студенту

Хорольському Євгену Віталійовичу

1. Тема роботи «Цифровий перетворювач звукових сигналів»
і керівник роботи Цибульский Леонід Юрійович, доцент, к.т.н.
затверджені наказом по університету від «__» _____ 2019 р., № _____
2. Термін подання студентом проекту «5» червня 2019 р.
3. Вихідні дані до проекту: пристрій шифрувальної охорони мовного контенту, що базується на використанні алгоритму шифрування DES; об'єм резидентної пам’яті програм 16 Кбт, напруга живлення, 5В.
4. Зміст розрахунково-пояснювальної записки: Анотація; вступ; побудова та функціонування пристрою шифрувальної охорони; розробка конструкторської документації на перетворювач звукових сигналів. Розробка функціональної та електричної схеми системи взаємодії з периферійними пристроями.
5. Перелік графічного матеріалу: функціональна схема системи взаємодії з периферійними пристроями, електрична схема системи взаємодії з периферійними пристроями; допоміжні графічні матеріали.
6. Дата видачі завдання _21.03.2019_р.__

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів виконання дипломної роботи	Строк виконання етапів роботи	Примітка
1	Огляд науково-технічної літератури по системам та методам шифрувальної охорони даних мовного контенту	21.03.2019–05.04.2019	
2	Методи захисту від несанкціонованного доступу до баз даних	06.04.2019–19.04.2019	
3	Принципи побудови пристроїв обробки та шифрування повідомлень мовного контенту	20.04.2019–25.04.2019	
4	Загальні принципи шифрувального перетворення повідомлень мовного контенту	26.04.2019–5.05.2019	
5	Розробка технічних вимог до системи взаємодії з периферійними пристроями при обробці даних у системі DES	6.05.2019–12.05.2019	
6	Розробка функціональної та електричної схеми системи взаємодії з периферійними пристроями.	12.05.2019–17.05.2019	
7	Розробка алгоритмів та програмного забезпечення системи взаємодії з периферійними пристроями	18.05.2019–24.05.2019	
8	Оформлення пояснювальної записки.	25.05.2019–28.05.2019	
9	Перевірка на тексту ПЗ на унікальність	3.05.2019	
10	Креслення плакатів з формулами та графіками, підготовка доповіді.	10.06.2019	
11	Підписання дипломної роботи	16.06.2019	
12	Захист дипломної роботи	20.06.2019	

Студент гр. ДЕз-41 _____ Є. В. Хорольський

Керівник проекту _____ Л.Ю. Цибульский

Р Е Ф Е Р А Т

Цифровий перетворювач звукових сигналів / Бакалаврська робота напряму підготовки **6.050802 – «Електронні пристрої та системи»** спеціалізації **«Електронні прилади та пристрої». Хорольський Євген Віталійович.** НТУУ «КПІ імені Ігоря Сікорського». Факультет електроніки, кафедра електронних приладів та пристроїв. Група ДЕ-з41. – К.: НТУУ «КПІ імені Ігоря Сікорського», 2019. – 77 с., іл. 19, табл. 10.

Ключові слова: ЗАХИСТ ІНФОРМАЦІЇ, ТЕХНОЛОГІЯ, СИСТЕМА, АЛГОРИТМ

Короткий зміст роботи: Дана дипломна робота присвячена дослідженню методів та засобів перетворювання даних мовного контенту, проведено аналіз відомих технічних рішень з питань охорони системи даних, переданих по каналах електрозв'язку, від стороннього доступу, приведено загальні принципи побудови пристроїв захищенного зв'язку; описано методи шифрування та основні поняття криптографії; приведено розробку технічних вимог до системи взаємодії з периферійними пристроями при обробці даних у системі, технічні вимоги, які висуваються до системи взаємодії периферійних пристроїв при обробці даних у стандарті DES, розробку функціональної схеми системи взаємодії з периферійними пристроями, розробку електричної схеми системи взаємодії з периферійними пристроями, описано алгоритм шифрування. В додатках приведено розробку програмного забезпечення та методику налагодження алгоритмічного і програмного забезпечення системи взаємодії з периферійними пристроями.

Отримані результати:

- розроблено пристрій шифрувальної охорони, що базується на використанні алгоритму шифрування DES, який дозволяє здійснювати обмін даними при використанні з пристроями різних виробників з аналогічним алгоритмом шифрування.

А Н О Т А Ц І Я

В даній роботі був розроблений пристрій шифрування повідомлень мовного контенту, який унеможливлює перехоплення комунікаційного повідомлення сторонніми особами. Цей пристрій кодування за рахунок шифрування засновано на використанні алгоритму шифрування DES, що дозволяє робити обмін контентом при використанні з пристроями різних виробників з аналогічним алгоритмом шифрування. При використанні пристрою криптоохорони в стандарті DES, оператор повинний знати, що теоретично при підборі кодів зловмисник може знайти правильний код без використання всіх комбінацій. Тому потрібно вживати заходів для охорони кодів.

S U M M A R Y

In this paper, the device encoding messages of linguistic content, which prevents interception of communication with third parties. This encryption device based on encryption is based on the use of the DES encryption algorithm that allows you to exchange content when used with devices of different manufacturers with a similar encryption algorithm. When using the crypto device in the DES standard, the operator should know that theoretically, when picking up codes, the attacker can find the correct code without using all combinations. Therefore, it is necessary to take measures to protect the codes.

ЗМІСТ

					ЗБР 6.050802.041 ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Хорольський Є.В.			Цифровий перетворювач звукових сигналів *Пояснювальна записка*	Літ.	Арк. 5 / Аркушів 73
Перевір.		Цибульский Л.					
Н. Контр.		Чадюк В.О.				КПІ, ФЕЛ, ДЕ-з41	
Затверд.		Писаренко Л.Д					

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

АДИКМ – адаптивна диференціальна імпульсно-кодова модуляція;

ІКМ – імпульсно-кодова модуляція;

ДМ – дельта-модуляція;

ЗШ – зняття шифру;

КЗ – канал зв’язку;

КШ – командами від шифроутворюючих пристроїв;

НШ – накладення шифру;

ПП – перетворюючого пристрою;

ПСКЗ – пристрої сполучення з каналом зв’язку;

ПУ – перетворюючого пристрою;

СІ – синхроімпульси;

СТЧ – сигнали тактової частоти;

СП – синхронізуючого пристрою;

СШ – синхронізатори шифратора-дешифратора;

ШМС – шифровані мовні сигнали;

ШП – шифроутворюючий пристрій;

СШ –системи шифрування – шифратора і дешифратора

DES – Data Encryption Standart – американський стандарт шифрування;

PMM – Power Management Mode – режим керування живленням;

Scrambler – скремблер, змішувач

ВВЕДЕННЯ

Стандарт безпеки даних мобільного контенту визначає засоби контролю проходження сигналів для забезпечення безпеки даних мовлення протягом усього терміну операції. Вимоги шифрування застосовуються до всіх каналів прийому-передачі мовного контенту.

Суб'єкти та постачальники послуг третіх сторін повинні працювати зі своїми користувачами, щоб зрозуміти свою відповідальність за дотримання норм і звітування. Це особливо актуально для юридичних осіб у місцях, де встановлені національні користувачі інтегрованих цифрових мереж та комутованих мобільних мереж зв’язку до ексклюзивного надання послуг. Ризики і вразливості, пов'язані з мобільними мережами обміну контентом, вимагають охорони незалежно від розміру або можливостей середовища комунікаційних мереж.

Особливе місце забезпечили собі роботодзвінки (Robocall), також відомі як "голосове мовлення", - це будь-який мобільний дзвінок, який передає попередньо записане повідомлення, використовуючи автоматичну (комп'ютеризовану) систему набору номеру користувача, більш часто згадувану як автоматичний номер або "автодозвон". Автодозвон або з'єднує виклик з живою особою, або відтворює попередньо записане повідомлення. Обидва вважаються роботодзвінками. Деякі роботодзвінки використовують персоналізовані звукові повідомлення для імітації фактичного особистого дзвінка. Закон забороняє роботодзвінкам з'єднуватися на:

- традиційні номери стаціонарних споживачів зв’язку;
- номери стаціонарних номерів;
- всі номери мобільних телефонів.

Роботодзвінки до стаціонарних телефонів бізнесменів законом не обмежені. Роботодзвінки користуються популярністю серед багатьох галузевих груп, таких як торгівля нерухомістю, телемаркетинг і компанії з прямих продажів. Більшість компаній, які використовують роботодзвінки, є законним бізнесом, але деякі не є. Ті незаконні підприємства можуть не просто дратувати

споживачів - вони також можуть намагатися їх обдурити. Для кращої охорони споживачів, особливо людей похилого віку та інших вразливих груп (наприклад, іммігрантів без хорошого розуміння мови) розробляються нові регулювання.

Обмін даними відіграє на тепер вирішальну роль в ході бізнес боротьби, у процесі технічного розвитку, на ринках будь якої. Боротьба за перевагу у науково-технічного прогресу в напрямках що зумовлюють цей прогрес. Конкуренція бізнесу, конкуренція політиків ставить учасників ринку в рамки, де не рахуються з вимогами моралі минулих сторіч, багатьом з учасників боротьби приходиться шукати переваги, займатися промисловим шпигунством.

У цих умовах таємна діяльність по добуванню, збору, аналізу, збереженню і продажу баз даних стає професійною. Це визначається тим, що одержання достовірних даних про цінні об'єкти легально неможливе внаслідок існування і підтримку визначеної системи охорони коштовних даних від кримінального, доступу з боку зловмисників. Тому робота присвячена розробці електронного пристрою, який би не просто перетворював звукові сигнали, а шифрував їх і тим самим би унеможливлював прослуховування розмов.

Інтерес до скритного одержання конфіденційних даних виявляється з давніх часів. В даний час створені технічні пристрої підслуховування для прослуховування бесід з дуже великої відстані, абсолютно безпечного з погляду тих хто розмовляє на вулиці, у парку, у саду і т.п. Робота таких приладів базується на використання мікрофонів спрямованої дії. Розробляється спеціальна конструкція і забезпечується чутливість електронними приладами з відмінними шумовими характеристиками. Також, використовують малошумлячі підсилювачі. Такі пристрої зазвичай використовуються для запису мови журналіста в натовпі, чи на природі, там, де до джерела звуку не можна підійти близько. Вони використовуються при виконанні рятувальних робіт для пошуку людей при обвалах на підземних об'єктах та будівель при землетрусах. Для скритного підслуховування конфіденційних бесід і розмов навмисно використовуються так називані "жучки", що являють собою мікрофон, сполучений з УКВ чи передавачем включений у лінію мобільного зв'язку чи електричну мережу. Навмисно переговори перехоплюють не тільки в

бездротових мережах, але і підключення дротів до мережі, а також індукційними датчиками чи ємнісними датчиками, які не вимагають контакту. Такі датчики установлюються в межі дії електромагнітного поля, яке випромінюють дроти ліній передачі. Далі здійснюється селекція радіотехнічними засобами, яких на сьогодні довга технологічна лінійка. Всі ділянки мережі мобільного зв'язку де поширюється сигнал можуть бути використанні для підслуховування звукового каналу легкодоступними засобами сучасної електроніки [1].

Найбільш уразливими для скритного доступу є мережі в системах мобільного бездротового зв'язку, супутникові і радіорелейні канали в незахищених приміщеннях, у житлових будинках, в яких розміщаються офіси компаній та організацій.

Підготовлені фахівці можуть легко здійснити перехоплення мобільного зв'язку чи знімання сигналів із проводів. Сьогодні підслуховування і перехоплення доступні навіть аматорам.

1 МЕТОДИ ПЕРЕТВОРЕННЯ СИГНАЛІВ У КОМУНІКАЦІЙНИХ КАНАЛАХ МОВНОГО КОНТЕНТУ

1.1 Методи охорони конфіденційних даних від стороннього доступу

Оцінювати важливість різного роду знань та важливість збереження їх в таємниці навчилися здавен. Знання часто стають скарбом дорожче золота, а володіння ними може забезпечити добробут, вплив і владу. Підраховано, що втрата банком 20-25% конфіденційних даних веде до його руйнування.

Інформація, яку необхідно сховати від сторонніх, по-англійськи називається sensitive (чутлива, яку необхідно охороняти), на відміну від офіційної має гриф секретності, яка по-англійськи називається classified. Методами приховування самого факту передачі повідомлення займається стеганографія (від грецьких слів stege- " дах " і grapho- " пишу "), в той час як методами шифрування або кодування повідомлення займається криптографія (від грецьких слів kryptos- " таємний ' 'і grapho -' 'пишу' ').

Дисципліна, що займається розкриттям шифрів, називається криптоаналізу, а криптографія і криптоаналіз разом називаються криптології. За загальноприйнятою термінології слово " конфіденційний " означає: довірчий, який не підлягає розголосу, секретний. Стосовно до теперішнього стану і призначення систем зв'язку всі види даних можна поділити на три групи:

а) секретні, б) конфіденційні, в) відкриті.

Секретні - це дані, які знаходяться під охороною держави від небезпечних організацій та осіб, збереження яких регламентовано, відповідними законами і за витік яких настає кримінальна відповідальність [2].

До конфіденційних можна віднести дані, які призначені для використання обмеженого кола осіб (наприклад: комерційні секрети, якими користуються довірені особи будь-якої фірми, банку і т.п.) і витік якої, хоча і не завдає державного шкоди, але може завдати значної шкоди певному колу осіб або фірм.

Використання відкритих даних зазвичай не обмежується. Забезпечення секретності переданих мобільними мережами мовних даних вимагає застосування складної апаратури засекречування (апаратура ЗАС) і строгих організаційних заходів (прокладка спеціальних кабелів зв'язку; контроль на відсутність "жучків" і побічних випромінювань; використання телефонних апаратів, комутаційної та іншої техніки в спеціально захищеному виконанні і т.п.), що призводить до великих матеріальних втрат на оснащення та експлуатацію мережі. Цим вимогам задовольняють мережі Урядової зв'язку, а також деякі відомчі мережі. Апаратура і пристрої для цих мереж створюються за технічними вимогами замовників, які здійснюють експлуатацію. Забезпечення тільки конфіденційності (без гарантії забезпечення секретності) вимагає значно менших матеріальних витрат і для переважної більшості користувачів мереж зв'язку є більш ніж достатнім. Очевидно, що запобігти випадкове або навмисне підслуховування (забезпечити конфіденційність) можна за допомогою досить простих в експлуатації пристроїв і без проведення дорогих організаційних і технічних заходів. Природно, що для пристрою конфіденційного зв'язку повинні бути сумісні і забезпечувати роботу по стандартних каналах зв'язку.

Розглянемо докладніше основні шляхи витоку даних через технічні засоби, а потім методи скремблювання і шифрування.

Під витоком даних розуміється їх одержання сторонньою особою випадково чи навмисно з використанням ними технічних засобів (у тому числі спеціальних) без інформування власників даних. Інакше це можна назвати стороннім доступом до контенту (СД). Одержання конфіденційних даних можливо трьома шляхами:

а) прямим підслуховуванням;

б) підслуховуванням з використанням пристроїв, аналогічних тим, що використовують власники інформації (наприклад: телефонний апарат, факс, ПЕВМ);

в) обробкою перехопленої інформації за допомогою спеціальних засобів і методів.

Відомо, що ланцюг проходження мовного контенту й інших видів інформації з бездротової мобільної мережі загального користування, складається з декількох ділянок:

1) користувацька ділянка,

2) ділянка місцевої мережі,

3) ділянка внутрішньої мережі,

4) ділянка магістральної мережі.

Останній є загальним для обох користувачів, що обмінюються мовною інформацією, а інші повторюються з боку кожного користувача. Канал тональної частоти (ТЧ), що з'єднує користувачів, має стандартну ширину смуги 0,3...3,4 кГц. При цьому на всіх ділянках, крім користувацького, по фізичних ланцюгах передається згрупований сигнал, що містить одночасно інформацію від різних пар користувачів. Однак на границях ділянок і усередині ділянки місцевої мережі там, де відбувається транзит по низькій частоті, по фізичному ланцюзі проходить той же сигнал, що і на користувацькій ділянці.

На міжміській мережі комутуються групові сигнали (у вузлах автоматичної комутації). На інших комутаційних станціях комутується канал ТЧ. У тому числі на кінцевих станціях, вузлових (районних АТС), центрових (вузли вихідних і вхідних повідомлень) і на автоматичних міжміських телефонних станціях (АМТС).

Де інде, де проходить комунікаційний сигнал звукової частоти, можливо прослуховування при прямому підключені за допомогою навушників чи слухавки. В інших вузлах мережі для підслуховування необхідно мати пристрої чи апаратуру, що розпізнають канал мовного з'єднання, які цікавлять.

У мережах мобільного зв'язку на користувацьких відрізках і в місцях комунікації, подібним транзитам ТЧ, замість каналу ТЧ може використовуватися основний цифровий канал - ОЦК (транзит по імпульсах на швидкості 64 кбіт/с). У цьому випадку в користувачів повинні бути технічні засоби (чи користувацькі комплекти) у який маються відповідні пристрої, що кодують, у тому числі аналогово-цифрові (АЦП) і цифро-аналогові (ЦАП) перетворювачі. Будемо називати такі технічні засоби цифровими. Аналогічне

устаткування необхідно мати при підслуховуванні, що можливо на тих же ділянках, що і на аналоговій мережі [3].

Майже всі технічні засоби мають канали побічного витоку інформації. Наприклад, при використанні звичайних технічних засобів коли начебто б відключені комунікаційні апарати, на користувацьких проводах, що виходять за межі приміщення, наявні електричні сигнали по який можна довідатися усе, що говориться в приміщенні. При використанні спеціальних технічних засобів можна створити додаткові шляхи витоку даних. Наприклад, помістити в цифровий комунікаційний апарат мініатюрний передавач і підключити його до мікрофонного ланцюга, з виходу такого передавача аналогові мовні сигнали можуть бути передані по ефіру чи по користувацьких сполучних лініях передачі на великі відстані.

Побічними каналами витоку інформації є також системи пожежної сигналізації, озвучення приміщень, освітлення і т.д. Варіантів таких пристроїв дуже багато. Існують також акустичні канали витоку інформації, проаналізувати їхній весь досить складно, і в цьому немає особою необхідності для подальшого розгляду в даній роботі.

У каналах мобільного зв’язку, наприклад при використанні бездротових апаратів у мережах мобільного радіочастотного зв’язку, для підслуховування необхідно мати радіоприймачі, що дозволяють настроїться на відповідну частотну смугу скануючи приймачі. Можуть використовуватися і звичайні побутові приймачі, якщо на їхньому вході включити конвертор (пристрій для переносу смуги в інший діапазон частот).

Всі основні методи охорони від витоку інформації можна умовно розділити на двох груп:

– організаційні чи організаційно-технічні;

– апаратні чи програмно-апаратні.

До першої групи відносяться такі міри як:

– охорона приміщень, де розміщається апаратура зв’язку (комутаційне устаткування, апаратура ущільнення і т.п.);

– використання приладів що виявляють пристрої, що підслуховують, при сторонньому підключенні до ліній зв’язку;

– використання кабелів у герметичній оболонці з контролем розгерметизації (поява витоку газового чи іншого наповнювача) при ушкодженні цієї оболонки;

– екранування кабелів і їх шумові перешкоди (частина жил кабелю використовується для передачі по них шумових сигналів з великим рівнем);

– прокладка кабелів у важкодоступних траншеях із пристроями сигналізації про проникнення в них;

– шумові перешкоди приміщень і будівельних конструкцій за допомогою спеціальних генераторів акустичних, електричних і вібраційних перешкод.

До другої ж групи можна також віднести такі методи, як:

– використання несучих подібних до шумових перешкод у каналах радіозв’язку, коли смуга частот переданих сигналів переміщається у використовуваному діапазоні частот по квазі-випадковому закону;

– використання в рухливому радіозв’язку стільникових структур, коли при переміщеннях користувача по території мережі змінюються частоти;

– використання систем типу обмеження доступу;

– використання пристроїв охорони від прослуховування;

– використання пристроїв виявлення знімання інформації.

Але варто відзначити, що за даними фахівців в області охороні розмовного контенту, що мається в продажі устаткування виявлення негласного знімання інформації з провідних каналів реагує лише на зміну імпедансу лінії зв’язку. Тому використання такого устаткування не може гарантувати його власнику надійна охорона від витоку інформації.

Організаційні й організаційно-технічні методи в ряді випадків є достатніми для охорони конфіденційної інформації. Однак, у ряді випадків, у комерційних мережах економічно вигідніше і більш надійно можна захиститься від витоку інформації шляхом використання апаратних (апаратура конфіденційного зв’язку) і програмно - апаратних (пристрою конфіденційного зв’язку) методів.

Найпростішим методом охорони є кодування мовних сигналів за законами, що відрізняється від загальноприйнятих (стандартних) [4].

В аналогових каналах для кодування може бути використана інверсія у всій смузі каналу ТЧ (інверсія - це перетворення спектра мови в заданій смузі частот, при якому нижні частоти стають верхніми, верхні - нижніми). Можливо також поділ каналу ТЧ на наскільки більш вузьких смуг, перенос їх по частоті і зрушення за часом відносно один одного. В останньому випадку буде відбуватися погіршення якості і розбірливості мови через утрати частини спектра мови при фільтруванні. У цифрових каналах для охорони інформації можуть використовуватися ті ж методи, що й у каналах ТЧ, а також зміна місця розташування кодових знаків у кодових комбінаціях. Закони кодування в розглянутих випадках залишаються незмінними, принаймні , протягом сеансу зв'язку. Такі методи, звичайно, називають простим кодуванням.

Більш складними і, відповідно більш надійними методами захисту є методи, при яких закони кодування змінюються в процесі передачі інформації. Такі методи називають динамічним кодуванням. У каналах ТЧ це інверсія, що комутується, частотні перестановки, тимчасові перестановки, а також комбінація цих методів. У цифрових каналах поряд з такими перетвореннями може здійснюватися перетворення цифрової послідовності шляхом чи перестановки заміни кодових знаків ("0" на "1" чи "1" на "0"). Сучасний рівень розвитку мікроелектроніки дозволяє навіть для каналів ТЧ здійснювати динамічне кодування мовних сигналів у цифровому виді. Мається на увазі, що аналоговий мовний сигнал після мікрофона перетвориться в цифровий, потім здійснюються необхідні зміни (фільтрація, перестановки, інверсія, і т.п.) і нарешті цифровий сигнал знову перетвориться в аналоговий, котрий передається по каналі ТЧ. На прийомному кінці декодування здійснюється аналогічним образом (у зворотному порядку).

При використанні розглянутих методів не усуваються деякі ознаки вихідного мовного сигналу в каналі зв'язку. При прямому прослуховуванні можна одержати корисну інформацію про що говорить і навіть зрозуміти окремі звуки, склади, слова і фрази. Тобто в каналі зв'язку може зберегтися

"залишкова" розбірливість мови чи такі ознаки, що дозволяють відновити вихідний сигнал за допомогою пристроїв типу "бачу мову" (спектрограф за допомогою якого виходить тривимірне зображення в координатах: час, частота, амплітуда).

У наукових джерелах електронні пристрої, що реалізують розглянуті перетворення, звичайно називають скремблерами. В останні роки розроблений ряд удосконалених мовних скремблерів, що забезпечують високу безпеку і прийнятну якість мови при не занадто складній конструкції. Розробка таких скремблерів стала можливою завдяки досягненням в області створення процесорів цифрової обробки сигналів.

У цифровому виді можуть передаватися мовні сигнали перетворені різними методами (імпульсно-кодова модуляція - ІКМ, дельта – модуляція - ДМ, адаптивна диференціальна ІКМ - АДИКМ і т.п.). Для охорони інформації цифрова послідовність у каналі зв’язку шифрується шляхом накладення на неї іншої квазівипадкової послідовності, сформованої за законом, обумовленому "ключем" (наприклад, додавання по модулю числа 2). У цьому випадку залишкова розбірливість у каналі зв’язку практично нульова, і немає необхідності використовувати "змішування" (скремблювання). Ступінь охорони інформації цілком визначається складністю "ключів" і паролів, використовуваних взаємодіючими користувачами, а також методами їхнього обміну в момент установлення з’єднання.

1.2 Принципи побудови пристроїв обробки та шифрування мовних повідомлень

1.2.1 Загальні принципи побудови пристроїв конфіденційного зв’язку

Пристрої конфіденційного зв’язку або пристрої охорони даних (засекречування) мобільних переговорів призначені для таких перетворень мовних сигналів, при яких користувачі, що знаходяться на кінцевих пунктах системи зв’язку, можуть вести переговори так само, як це відбувається в звичайних комунікаційних мережах, але в той же час розбірливість мови в

каналах і лініях зв’язку (залишкова розбірливість) дуже мала, а в граничному випадку дорівнює нулю.

При застосуванні існуючих технічних засобів перехоплення й обробки сигналів з використанням самої швидкодіючої обчислювальної техніки можливо розкрити зміст переговорів, однак зробити це досить важко, а в деяких випадках практично чи неможливо потрібно багаторічна робота..

Структурні схеми усіх відомих пристроїв охорони даних можна звести до двох різновидів, показаним на рис.1.1.

Інформаційний сигнал надходить на вхід перетворюючого пристрою (ПУ). Необхідні для роботи цього пристрою тактові частоти й інші допоміжні сигнали (СТЧ) надходять від синхронізуючого пристрою (СП), що керує також роботою інших вузлів схеми.

Шифроутворюючи пристрої (ШП) виробляють сигнали необхідні для забезпечення засекречування мовних сигналів, а також синхроімпульси (СІ), необхідні для забезпечення синхронної і синфазної роботи приймальної і передавальної частин апаратури. Синхроімпульси встановлюють шифроутворюючи й інші пристрої у початковий стан.

По каналу зв’язку (КЗ) передаються зашифровані мовні сигнали (ШМС), сигнали, що синхронізують роботу шифратора і дешифратора (СШ), сигнали необхідні для синхронізації мовоперетворюючих пристроїв і тактових частот.

Об’єднання цих сигналів для передачі по каналі зв’язку і їхній поділ здійснюється в пристроях сполучення з каналом зв’язку (ПСКЗ).

Алгоритм роботи перетворюючого пристрою (ПП) на рис.1.1(а) змінюється за командами від шифроутворюючих пристроїв (КШ). У схемі рис.1.1,б алгоритм роботи ПП не змінюється, а в канал зв’язку надходить сукупність мовних сигналів і сигналів від шифроутворюючого пристрою. Ця сукупність у вузлі накладення шифру (НШ), може формуватися різними методами (додавання, перемножування і т.п.). Зворотне перетворення відбувається у вузлі зняття шифру (ЗШ).

Ступінь охорони даних чи як її іноді називають "стійкість засекречування" у схемах рис.1.1 визначається роботою двох пристроїв: шифроутворюючого і перетворюючого [5].

Під стійкістю засекречування можна розуміти здатність протистояти сторонньому доступу до переданого по каналі зв’язку контенту. Одним з основних критеріїв при оцінці стійкості засекречування є відношення тривалості часового інтервалу, необхідного для розкриття контенту стороннім суб'єктом до тривалості вихідного повідомлення. Звичайно здобуттям скритих даних, розкриттям інформації займаються фахівці, яких називають дешифрувальниками. Передбачається, що дешифрувальник має доступ до каналу зв’язку і може записати передане зашифроване повідомлення для наступної багаторазової обробки, використовує самі зроблені ЕОМ, йому відома схема і параметри апарата, що засекречує, (чи він має цей апарат), однак він не знає "ключа" введеного в шифроутворюючий пристрій.

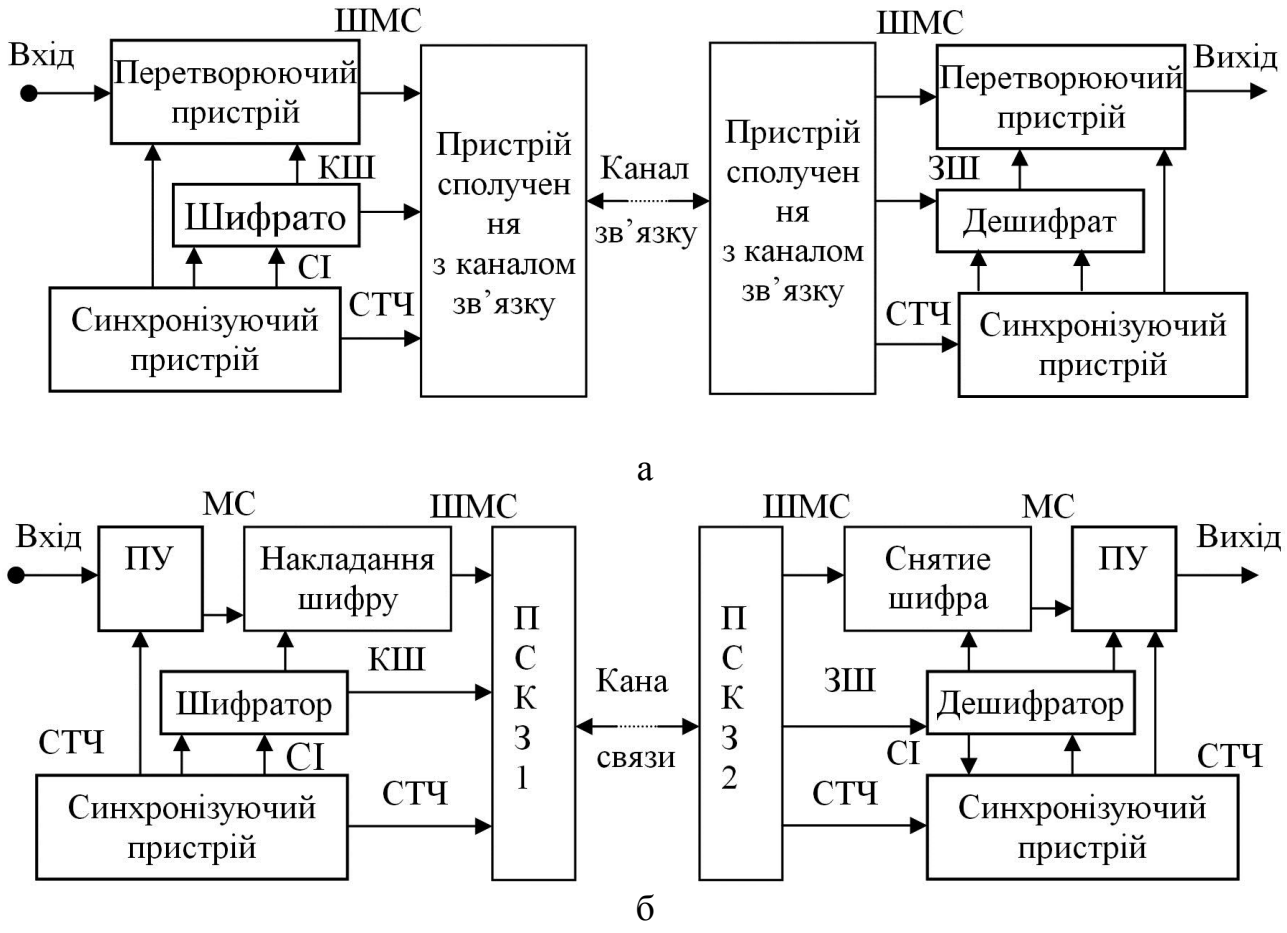

Рисунок 1.1 – Структурні схеми пристрою охорони мовних сигналів

Пристрої утворення шифру можуть забезпечити практично будь-яку задану стійкість засекречування. Підвищення стійкості досягається звичайно за рахунок ускладнення схемно-технічних рішень і, отже, приводить до збільшення вартості устаткування. З огляду на це, при проектуванні шифроутворюючих пристроїв стійкість засекречування задають з урахуванням техніко-економічних характеристик.

При використанні схеми рис.1.1,а зашифрований сигнал у каналі зв'язку зберігає ряд властивостей вихідних сигналів. Наприклад, при перетвореннях мовних сигналів у каналі зв'язку будуть міститися більш-менш виражені такі ознаки, як: частота основного тону і її гармоніки, місце розташування частот формант і т.п. Використовуючи ці ознаки і статистичні властивості мовних сигналів, можна здійснити дешифрування без аналізу шифроутворюючого пристрою і без визначення "ключа". У цих випадках при як завгодно високій шифрувальній стійкості шифратора, стійкість засекречування мови може бути щодо невисокої і буде цілком визначатися стійкістю алгоритмів перетворення мови.

Стійкість засекречування, обумовлена зміною алгоритмів перетворень мовних сигналів, для більшості відомих типів мовоперетворюючих пристроїв також може бути оцінена на основі досить строгих критеріїв і методів. Підвищення стійкості засекречування також, як і для шифроутворюючих пристроїв, приводить до ускладнення технічних рішень. При цьому, як правило, при ускладненні алгоритмів перетворень погіршується якість і розбірливість мовних сигналів на виході пристрою, що дешифрує. Тому одержати дуже високу стійкість засекречування за рахунок ускладнення алгоритмів перетворення мовних сигналів практично неможливо.

При використанні схеми рис.1.1,а практично неможливо домогтися усунення ознак вихідних сигналів у каналі зв'язку і відповідно стійкість засекречування відносно невисока. Однак, з огляду на, що технічна реалізація подібної схеми звичайно більш проста, а також те, що в ряді випадків досить

зберегти конфіденційність переданої інформації в плині обмеженого часу, схема рис.1.1,а має досить широке застосування.

Використання схеми рис.1.1,б дозволяє цілком позбутися від наявності ознак вихідних мовних сигналів у каналі зв'язку. Це можна зробити, наприклад, перетворивши мовні сигнали, що надходять на вузол накладення шифру (НШ), у двійкові імпульси. Стійкість засекречування в цьому випадку може бути як завгодно високої і визначається шифрувальною стійкістю шифроутворюючих пристроїв.

Слід зазначити, що при сучасному рівні розвитку мікроелектроніки і цифрових методів обробки сигналів, у всіх типах пристроїв охорони даних, у тому числі мовних, всі основні перетворення сигналів, як правило, здійснюються в цифровому виді. При цьому в ПП спочатку стоїть аналогово-цифровий перетворювач (АЦП), потім проводиться обробка цифрових сигналів. На виході ПП може бути включений цифро-аналоговий перетворювач (ЦАП) і в канал зв'язку при цьому надходять аналогові сигнали.

У загальному випадку шифратори, перевершуючи скремблери по складності, мають більш високу стійкість засекречування. Двійкова послідовність зовсім не розрізняється людським вухом. Перетворена в цифрову форму мову звучить подібно безупинному вереску. Двійкова послідовність пропускається через блок шифрування, що змінює її відповідно до математичної формули, відомої тільки учасникам засекреченого зв'язку. Дешифрувати зашифровану розмову, не володіючи ключем шифрування, практично неможливо, оскільки число можливих варіантів ключів майже безмежно.

Аналогові сигнали "засекречені" скремблером можна прослухувати "неозброєним" вухом. Для непрофесійного слухача заскремблована мова буде звучати подібно іноземній мові, але для того, хто знає, як перетворити шифротекст у відкритий, вона буде осмисленою.

Застосовані кодові комбінації можуть бути відновлені спеціально підготовленими аналітиками, навченими розпізнаванню й інтерпретації засекреченої за допомогою скремблерів мови. Більш того, спеціалізоване

лабораторне устаткування для електронного аналізу дозволяє легко розкривати засекречений аналоговий сигнал, оскільки кількість можливих комбінацій при скремблюванні менше, ніж при цифровому зв'язку.

Переваги цифрового методу шифрування над аналоговим (частотно-часовими перестановками) зведені в табл..1.1.

Таблиця 1.1

	Аналоговий	Цифровий
Наявність переговорів в лінії зв'язку	Є виразні ознаки	Немає ніяких ознак, тому що в лінію йде чистий шифр (лінійний режим)
Розподіл амплітуди сигналу	Є ритм і голосність	У каналі зв'язку однорідна двійкова послідовність
Постійне шифрування в 4-х провідному каналі зв'язку	Неможливо	Можливо
Короткочасний спектр сигналу	Спектральні характеристики однорідні	Спектральні характеристики неоднорідні

1.2.2 Загальні принципи шифрувального перетворення мовних повідомлень

Розглянемо загальні принципи шифрувального перетворення мовних повідомлень (див. рис. 1.2).

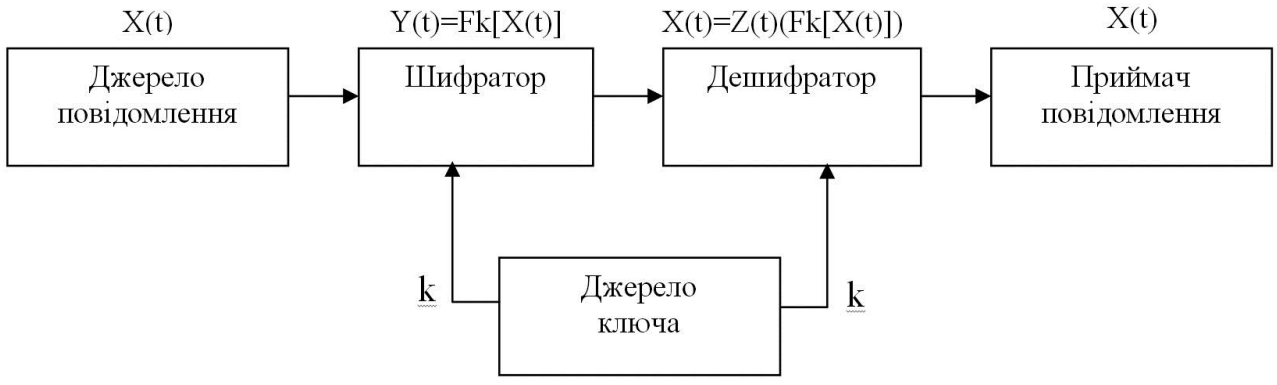

Рисунок 1.2 – Принципи шифрувального перетворення мовних повідомлень

Будемо називати вихідне мовне повідомлення, що передається по радіо чи провідному каналу, відкритим повідомленням і позначати X(t).Це повідомлення надходить у пристрій шифрувального перетворення (шифрування), де формується зашифроване повідомлення Y(t) за допомогою наступної залежності:

$$Y(t) = Fk[X(t)],$$

де Fk[.] - шифрувальне перетворення; k - ключ шифрувального перетворення,

Тут під ключем шифрувального перетворення будемо розуміти деякий параметр k, за допомогою якого здійснюється вибір конкретного шифрувального перетворення Fk[.]. Очевидно, що чим більше потужність використовуваної безлічі ключів шифрувального перетворення k, тим більшому числу шифрувальних перетворень може бути піддане мовне повідомлення X(t), а, отже, тим більше невизначеність у зловмисника при визначенні використовуваного в даний момент шифрувального перетворення Fk[.].

При шифруванні повідомлення X(t) повинні використовуватися такі шифрувальні перетворення, при яких ступінь охорони даних розмовного контенту визначався б тільки потужністю безлічі ключів шифрувального перетворення k.

Зашифроване повідомлення Y(t) передається по радіо чи провідному каналу зв’язку. На прийомній стороні це повідомлення розшифровується з метою відновлення відкритого повідомлення за допомогою наступної залежності:

$$X(t) = Zk[Y(t)] = Zk\{Fk[X(t)]\},$$

де – Zk [.] - зворотне по відношенню Fk [.] перетворення.

Таким чином, наявність в користувачів однакових ключів k і шифрувальних перетворень Fk [.], Zk [.] дозволяє без особливих складностей здійснювати зашифрування і розшифрування мовних повідомлень.

Очевидно, що для розгляду способів шифрувального перетворення мовних повідомлень необхідно мати представлення про ті процеси, що лежать в основі формування цих повідомлень.

Мовний контент комунікується електричними сигналами після перетворення мікрофоном комунікаційного апарата акустичних сигналів в електричні. Надалі здійснюється посилення цих сигналів до необхідного рівня. На стороні абонента в комунікаційному апараті електричні сигнали піддаються обробці і зворотному перетворенню в звукові сигнали.

Основні характеристики звукового повідомлення: тривалість X(t), амплітудно-частотний спектр S(f). Тим самис повідомлення X(t) представляється або у часовій області, або у частотній.

Для визначення з часового і частотного представлень мовного контенту X(t) мобільного або дротового повідомлення використовуються шифрувальні перетворення самого повідомлення X(t) або його амплітудно-частотного спектра S(f).

Помітимо, що вухо людини, в залежності від розвитку, сприймає звукові сигнал від 15 Гц до 20 кГц. Для того, щоб зберегти пізнавальність голосу користувача по тембрі, чистоту і гарну роздільність звуків можливо передавати звуковий сигнал у іншому частотному діапазоні. З практики відомо, для розпізнання голосу достатньо передавати сигнали в межах частотного діапазону 300 – 3400 Гц. Саме такі діапазони частот передачі мають стандарти мобільної і дротової передачі мовного контенту у світі.

Шифрувальні перетворення за параметром стійкості розділяють на дві самостійні груп.

До першої групи відносяться стійкі до обчислювання і стійкі до розпізнання шифрувальні перетворення, а другу - безумовно стійкі шифрувальні перетворення.

Стійкі до обчислювання і стійкі до розпізнання відносяться шифрувальні перетворення, стійкість яких визначається обчислювальною складністю рішення деякої складної задачі. Основна розбіжність між цими шифрувальними перетвореннями полягає в тім, що в першому випадку маються підстави вірити,

що стійкість еквівалентна складності рішення важкої задачі, тоді як у другому випадку відомо, що стійкість, принаймні, велика. При цьому в другому випадку повинен бути наданий доказ, що розкриття переданого зашифрованого повідомлення Y(t) еквівалентно рішенню складної задачі.

Прикладом обчислювально стійких шифрувальних перетворень є складні шифрувальні перетворення, складені з великого числа елементарних операцій і простих шифрувальних перетворень таким чином, що зловмиснику для дешифрування перехопленого повідомлення Y(t) не залишається нічого іншого, як застосувати метод тотального випробування можливих ключів шифрувального перетворення, чи, як ще називають, метод грубої сили. За допомогою таких шифрувальних перетворень представляється можливим забезпечити гарантовану охорону переданого повідомлення X(t) від стороннього доступу.

До обчислювально стійких шифрувальних перетворень представляється можливим віднести і такі шифрувальні перетворення, при використанні яких зловмиснику для скритого доступу до повідомлення X(t) потрібно використовувати лише визначені алгоритми обробки повідомлення Y(t). Ці шифрувальні перетворення здатні забезпечити лише тимчасову стійкість.

До безумовно стійкого відносяться шифрувальні перетворення, стійкість яких не залежить ні від обчислювальної потужності, ні від часу, якими може володіти зловмисник. Тобто такі шифрувальні перетворення, що мають властивість не надавати зловмиснику при перехопленні повідомлення Y(t) додаткової інформації щодо переданого мовного повідомлення X(t).

Помітимо, що безумовно стійкі шифрувальні перетворення реалізувати дуже складно і тому в реальних системах мовного зв’язку вони не використовуються.

1.2.3 Шифрувальне перетворення аналогових мовних повідомлень

Найбільш простим і розповсюдженим способом шифрувального перетворення аналогових мовних повідомлень є розбивка повідомлень X(t) на частині і видача цих частин у визначеному порядку в канал зв'язку.

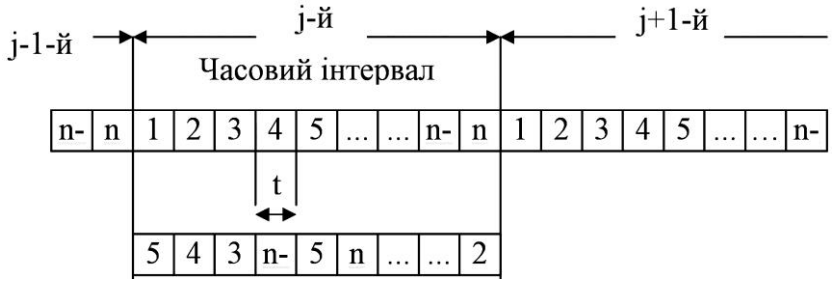

Рисунок 1.3 – Часові перестановки частинповідомлення X(t)

Цей спосіб полягає в наступному. Тривалість повідомлення X(t) (див. рис.1.3) поділяється на визначені, рівні по тривалості тимчасові інтервали T. Кожен такий часовий інтервал додатково поділяється на більш дрібні тимчасові інтервали тривалістю t. При цьому для величини n=T/t , як правило, виконується умова n = m ...10m , де m - деяке ціле число, m <10. Частини повідомлення X(t) на інтервалах часу t записуються в запам'ятовуюче пристрій, "перемішуються" між собою у відповідність із правилом, обумовленим ключем шифрувального перетворення k, і у виді сигналу Y(t) видаються в канал зв'язку. На прийомній стороні каналу зв'язку, де правило перемішування відомо, тому що мається точно такий же ключ шифрувального перетворення k, здійснюється "зборка" з повідомлення Y(t) відкритого повідомлення X(t) [2].

До переваг цього способу шифрувального перетворення відноситься його порівняльна простота і можливість передачі зашифрованого мовного повідомлення по стандартних мовних каналах. Однак цей спосіб дозволяє забезпечити лише тимчасову стійкість. Це наступним. Оскільки відкрите мовне повідомлення X(t) є безупинним, то в зловмисника після запису повідомлення Y(t) і виділення інтервалів тривалістю t (останнє досить легко зробити, тому що в каналі зв'язку присутня синхронізуючий сигнал) з'являється принципова можливість дешифрування повідомлення Y(t) навіть без знання використовуваного ключа k. З цією метою необхідно здійснити вибір інтервалів

таким чином, щоб забезпечувалася безперервність одержуваного повідомлення на стиках цих інтервалів. Очевидно, що при ретельній і кропіткій роботі з використанням спеціальної техніки можна досить швидко забезпечити таку безперервність, виділивши тим самим відкрите повідомлення X(t).

Тому такий спосіб шифрувального перетворення відкритих мовних повідомлень доцільно застосовувати тільки в тих випадках, коли інформація не представляє особливої чи цінності коли її цінність губиться через відносно невеликий проміжок часу.

Більш надійна охорона від стороннього скритого доступу можна забезпечити, якщо ідею розглянутого способу поширити на частотний спектр повідомлення X(t). У цьому випадку смуга пропущення мовного каналу F поділяється за допомогою системи смугових фільтрів на n частотних смуг шириною D f, що перемішуються відповідно до деякого правила, обумовленим ключем шифрувального перетворення k. Перемішування частотних смуг здійснюється зі швидкістю V циклів у секунду, тобто одна перестановка смуг триває 1/V с, після чого вона заміняється наступної.

Для підвищення надійності охорони від стороннього доступу після перемішування частотних смуг може здійснюватися інверсія частотного спектра повідомлення Y(t).

Розглянутий спосіб дозволяє забезпечити більш високий рівень охорони мобільного контенту від стороннього доступу в порівнянні з попереднім способом. Для відновлення відкритого повідомлення X(t) у цьому випадку зловмиснику необхідно мати додаткові дані по відносних частотах появи звуків і їхніх сполучень у розмовній мові, частотним спектрам дзвінких і глухих звуків, а також формантній структурі звуків. У табл.1 приведені дані по відносних частотах появи деяких звуків і границям формантних областей звуків російської мови, що можуть бути використані зловмисником при відновленні перехоплених мовних повідомлень.

Таблиця 1

Звук	Відносна частота появи, Гц	1-а формантна область, Гц	2-а формантна область, Гц
Голосний			
а	0,079	1100 - 1400	-
і	0,089	2800 - 4200	-
о	0,11	400 - 800	-
у	0,026	200 - 600	-
и	0,022	200 - 600	1500 - 2300
е	0,002	600 - 1000	1600 - 2500
Приголосний			
з	0,016	0 - 600	4200 - 8600
ж	0,008	200 - 600	1350 - 6300
л	0,04	200 - 500	700 - 1100
м	0,031	0 - 400	1600 - 1850
н	0,069	0 - 400	1500 - 3400
р	0,05	200 - 1500	-
с	0,054	4200 - 8600	-
ф	0,001	7000 - 12000	-
х	0,012	400 - 1200	-
ш	0,008	1200 - 6300	-

Очевидно, що найбільш високий рівень охорони мобільного контенту від стороннього доступу представляється можливим забезпечити шляхом об’єднання розглянутих способів. При цьому тимчасові перестановки будуть руйнувати значеннєвий лад, а частотні перемішувати голосні звуки.

Пристрою, що реалізують розглянуті способи, називаються скремблерами. У цьому зв’язку становить визначений інтерес серія скремблерів, у якості базового для який був використаний скремблер SCR - M1.2. Ці скремблери реалізують розглянуті способи шифрувального перетворення аналогових мовних повідомлень і досить широко використовуються в різних державних і комерційних структурах. У табл.1.2 приведені основні характеристики деяких скремблерів цієї серії.

Таблиця 1.2 Основні характеристики деяких скремблерів серії SCR - M1.2

Скремб-лер	Режим роботи	Ідентифікація користувача	Уведення сеансового ключа	Потуж-ність безлічі ключів	Габарити, мм	Вага, кг	Живлення
SCR-M1.2	Дуплексний зв'язок	Передбачена	Методом відкритого поширення ключів	2x1018	180x270x40	1,5	22В 50 Гц
SCR-M1.2 mini	Дуплексний зв'язок	Передбачена	Методом відкритого поширення ключів	2x1018	112x200x30	0,8	Від мережного адаптера 9-15 В, чи батарейного блоку
SCR-M1.2 multi	Дуплексний зв'язок	Може бути передбачена за бажанням замовника.	Методом відкритого поширення ключів	2x1018	180x270x45	1,6	220 В50 Гц

1.2.4 Шифрувальне перетворення цифрових мовних повідомлень

На практиці для перетворення мовного повідомлення X(t) у цифрову форму на передавальній стороні і відновлення цього повідомлення на прийомній стороні використовуються мовні кодеки, що реалізують один із двох способів кодування мовних повідомлень: форми і параметрів.

Основу цифрової комунікаційної мережі в даний час складає кодування форми повідомлень, кодування параметрів чи повідомлень, як називають, вокодерная зв'язок використовується значно рідше. Це визначається тим, що кодування форми сигналу дозволяє зберегти індивідуальні особливості людського голосу, задовольнити вимоги не тільки до розбірливості, але і до натуральності мови.

При кодуванні форми сигналу широко використовуються імпульсно-кодова модуляція (ІКМ), диференціальна ІКМ і дельта-модуляція.

Коротко розглянемо принципи здійснення ІКМ, диференціальної ІКМ і дельта-модуляції.

Рисунок 1.4 Узагальнена схема системи з ІКМ

Мовне повідомлення X(t) тривалістю T, що має обмежений частотою fm спектр, після фільтрації перетвориться в послідовність вузьких імпульсів X(l) = X(ID t), I =1,N, де N = T/D t, D t = 1/2fm, модульованих по амплітуді. Отримані миттєві значення X(I), I=1,N, квантуються по величині з використанням рівномірної, нерівномірної чи адаптивно-змінної шкали квантування. Квантування значення звітів Хкв(I), I=1,N, за допомогою кодера перетворяться в кодові слова, які характеризуються числом двійкових символів, що видаються в канал зв'язку.

На прийомній стороні кодові слова за допомогою декодера перетворяться в значення звітів Хкв(I), I=1,N, з яких за допомогою фільтра нижніх частот здійснюється відновлення повідомлення X(t).

Диференціальна ІКМ і дельта-модуляція відрізняються від ІКМ тем, що в них використане нелінійне відстеження переданого мовного повідомлення.

При цьому диференціальна ІКМ відрізняється від простий ІКМ тим, що квантуванню піддаються не самі відрахунки мовного повідомлення X(I), I=1,N, а різниця між відповідним відліком X(I) і результатом пророкування Хпр(I), формованим на виході провісника. При цьому в канал зв'язку видаються кодові слова, що містять коди цієї різниці і її знака (полярності). І, нарешті, дельта-модуляція відрізняється від простий ІКМ тим, що в канал зв'язку видаються тільки коди знака (полярності) у виді послідовності імпульсів, тимчасове

положення яких дозволяє відновити на прийомній стороні передане мовне повідомлення X(t), наприклад, за допомогою інтегратора.

Необхідно відзначити, що диференціальна ІКМ є найбільш кращої при формуванні цифрових повідомлень. Це обумовлено, в основному, тим, що використання диференціальної ІКМ дозволяє скоротити довжину кодових слів, тому що передачі підлягає тільки інформація про знак і величину збільшення. Крім того, використання диференціальної ІКМ дозволяє виключити перевантаження по крутості, з яким приходиться зіштовхуватися при лінійній дельта-модуляції.

У системах синтетичного чи вокодерного зв'язку по комунікаційному каналу передаються дані про деформації периферичного голосового апарата що говорить. Прийомний пристрій у таких системах являє собою модель голосового апарата людини, параметри якого змінюються відповідно до прийнятих даних. При цьому число параметрів, що характеризують голосовий апарат, порівняно невеликий (10...20) і швидкість їхньої зміни порівнянна зі швидкістю вимови фонем. У російської мови число фонем приймають рівним 42 і вони являють собою еквівалент виключаючи друг друга різних звуків.

Якщо вважати, що фонеми вимовляються незалежно з однаковою імовірністю, то ентропія джерела буде дорівнює log2 42 = 5,4 біт/фонему. У розмовній мові за одну секунду вимовляється до 10 фонем, тому швидкість передачі інформації не буде перевищувати 54 біт/с. З огляду на статистичний зв'язок між фонемами внаслідок надмірності мови, представляється можливим знизити швидкість передачі інформації до 20...30 біт/с.

Система вокодерного зв'язку функціонує в такий спосіб. У передавальній частині системи здійснюється аналіз мовного повідомлення X(t), що надходить з мікрофона, з метою виділення значень параметрів, що описують сигнал порушення, а також характеризують резонансну структуру мовного тракту. Значення параметрів у цифровому коді і передаються по каналі зв'язку. На прийомній стороні здійснюється синтез повідомлення X(t) з використанням прийнятих значень параметрів.

Таким чином, як при використанні кодування форми сигналу за допомогою ІКМ, диференціальної ІКМ і дельта-модуляції, так і при кодуванні параметрів у канал зв'язку видаються послідовності символів.

Отже, до цих послідовностей можуть бути застосовані відомі і досить широко використовувані на практиці шифрувальні перетворення й алгоритми.

В даний час найбільш відомими шифрувальними алгоритмами, що забезпечують гарантований рівень охорони переданих цифрових повідомлень від стороннього доступу, є американський стандарт шифрування даних DES (Data Encryption Standart), що прийнятий як федеральний стандарт США, і російський стандарт ДОСТ - 28147 - 89.

1.2.5 Алгоритм шифрування DES

Алгоритм засекречування даних розроблений для шифрування і дешифрування блоків даних, що складаються з 64 біт, при впливі на них ключа, також 64 біта [6].

Дешифрування здійснюється за допомогою того ж самого ключа, що використовується для шифрування, але з адресацією біт, видозміненої так, щоб дешифрування було б зворотним процесу шифрування.

Блок, що повинний бути зашифрований, спочатку піддається початковим перестановкам IP, потім складному перерахуванню, що залежить від ключа, і наприкінці , перестановкам IP-1, що є інверсними початковим перестановкам.

Перерахування, що залежить від ключа, може бути визначене як перетворення відповідно до функції шифрування f, функцією розподілу ключів KS.

На рис. 1.5 приведена структурна схема алгоритму шифрування.

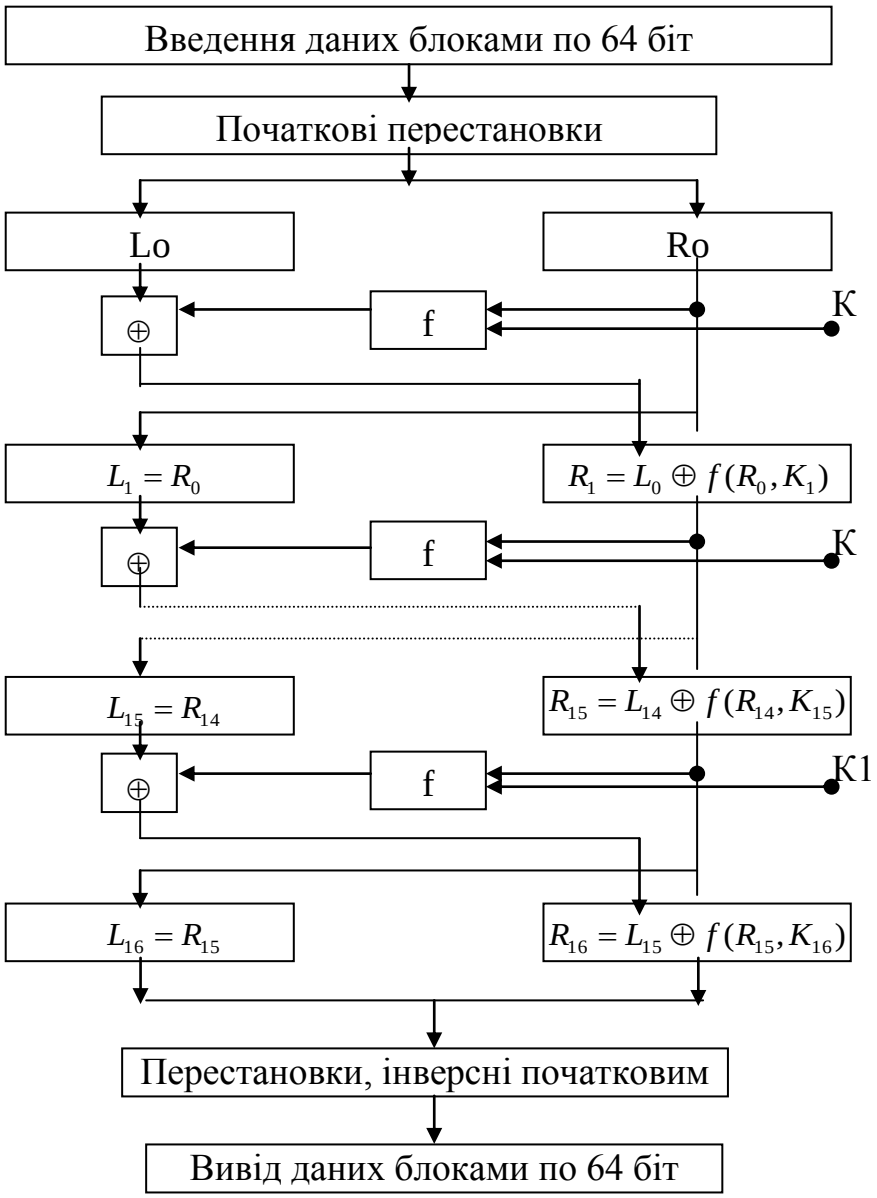

Рисунок 1.5 – Алгоритм шифрування DES

Введення даних виробляється блоками по 64 біта. Спочатку виробляються перестановки відповідно до таблиці 1.2.

Таблиця 1.2. Початкові перестановки (IP).

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

При цьому, наприклад, 58-ий інформаційний біт вхідного блоку вийде як перший, 50-й як другий, 2-й біт вийде 8-им, 1-й біт- 40-им.

Потім вхідний блок з переставленими бітами надходить на схему перерахувань, що складається з 16 послідовно включених вузлів - повторювачів (перетворення в кожнім з них повторюють попередні).

Тут інформаційний блок (64 біта) розбивається на дві частини L і R по 32 біта, що надходять на два входи повторювача. Вхідний блок тепер може бути позначений як LR. На третій вхід повторювача надходять блоки K по 48 біт зі схеми утворення "ключа". Блоки R і K обробляються за законом, що задається шифрувальною функцією f(R,K). Кожен біт отриманого блоку довжиною 32 біта складається по модулі два з бітами блоку L.

При цьому вихідні блоки L’ і R’ повторювача при вхідних блоках L і R і ключі До будуть рівні:

$$L'=R$$

$$R'=L \ (+) \ f(R,K)$$

де (+)- позначає додавання по модулі два інформаційних біти, що надходять з одного й іншого напрямку.

Алгоритм обчислення f(R,K) приведений на рис.1.6.

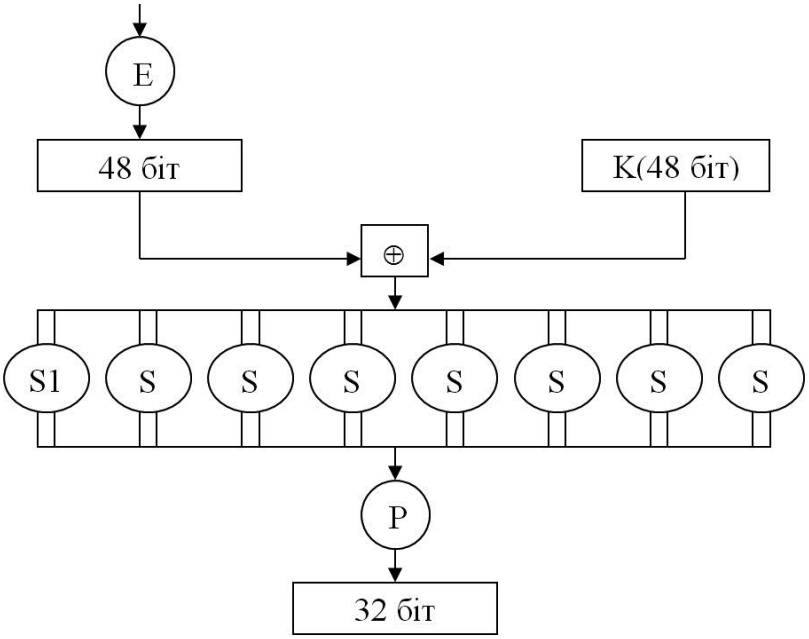

Рисунок 1.6 Обчислення f(R,K)

Тут E - функція яка перетворить 32 біта (на вході) у 48 біт (на виході). 48 біт виходу (8 блоків по 6 біт) виходять вибором бітів (вхідних) відповідно до таблиці 1.3.

Таблиця 1.3 "E"(Таблиця бітового вибору)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Далі функція Sn 6 біт (на вході) перетворить у 4 біти (на виході).

Розглянемо це перетворення на прикладі функції S1:

Рядок	Номер стовпця															
№	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	13	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	3

Якщо S1 - функція визначена в цій таблиці і B - блок з 6 біт, то S(B) визначаються: перший і останній біти в блоці B в двійковій системі представляють число в області 0-3. Нехай це число дорівнює i. Середні 4 біти в блоці "B" в двійковій системі представляють число в області 0-15. Нехай це число дорівнює j. Знайдемо в таблиці число в i-той колонці і j-тім стовпці. Це число в області від 0 до 15 і в двійковій системі представляється 4-х бітовим блоком. Цей блок є виходом S1 для введеного B. Наприклад, якщо B=011011, то номер стовпчика дорівнює 1 (01B), номер стовпця 13 (1101B). По таблиці знаходимо а колонку 1 і стовпці 13 число 5, тобто на виході число 0101. Функції S1,S2...S8 приведені в таблиці 1.4.

Таблиця 1.4 Функції S1…S8

S1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S4															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S5															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	4	2	3	6	15	0	9	10	4	5	3
S6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11

10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S7															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Функція перестановки P визначається таблицею 1.5.

Таблиця 1.5 Функція перестановки P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Вихідне значення P(L) для P визначеного цією таблицею виходить у такий спосіб: із блоку L береться 16-й біт L як перший біт P(L), 7-й біт як другий біт P(L), і так далі поки 25-й біт L не узятий як 32-й біт P(L).

Тепер нехай S1,...,S8 будуть вісім функцій вибору, P - функція перестановки і нехай E буде функція визначена вище.

Для того, щоб визначати f(R,K) ми спочатку визначаємо B1,...,B8 (по 6 бітів кожний):

$$B1B2...B8 = K(+)E(R) \quad (1.1)$$

блок f(R,K) потім визначається:

$$P(S1(B1)S2(B2)...S\,8(B8)) \quad (1.2)$$

У такий спосіб K(+)E(R) спочатку розділяється на 8 блоків як зазначене в (1.1). Потім кожен Bi узятий як введення в Si і 8 блоків (S1(B1)S2(B2)...S8(B8) по 4 біти кожне перетворюються в 1 блок 32 біта, що вводиться в P. Вихід P (1.2) є потім виходом функції f для введень R і K.

Прийнято, що KS (n, KEY) є функція, що визначається цілим числом n, що змінюється від 1 до 16 (n- номер повторювача) ключем (KEY) з 64 біт. Алгоритм обчислення Kn приведений на рис.1.7. Розглянемо алгоритм одержання функції KS. Спочатку 64 біт ключа піддаються перестановці PC-1 (табл.1.6).

Таблиця 1.6 Додаткові перестановки PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Таблиця розділена на дві частини, у першій частині вибираються біти C0 , у другій - біти D0. Біти ключа перераховані з 1 по 64. Біти C0 є відповідно бітами 57, 49, 41,..., 44 і 36 ключа, біти D0, є бітами 63, 55, 47,..., 12 і 4ключа.

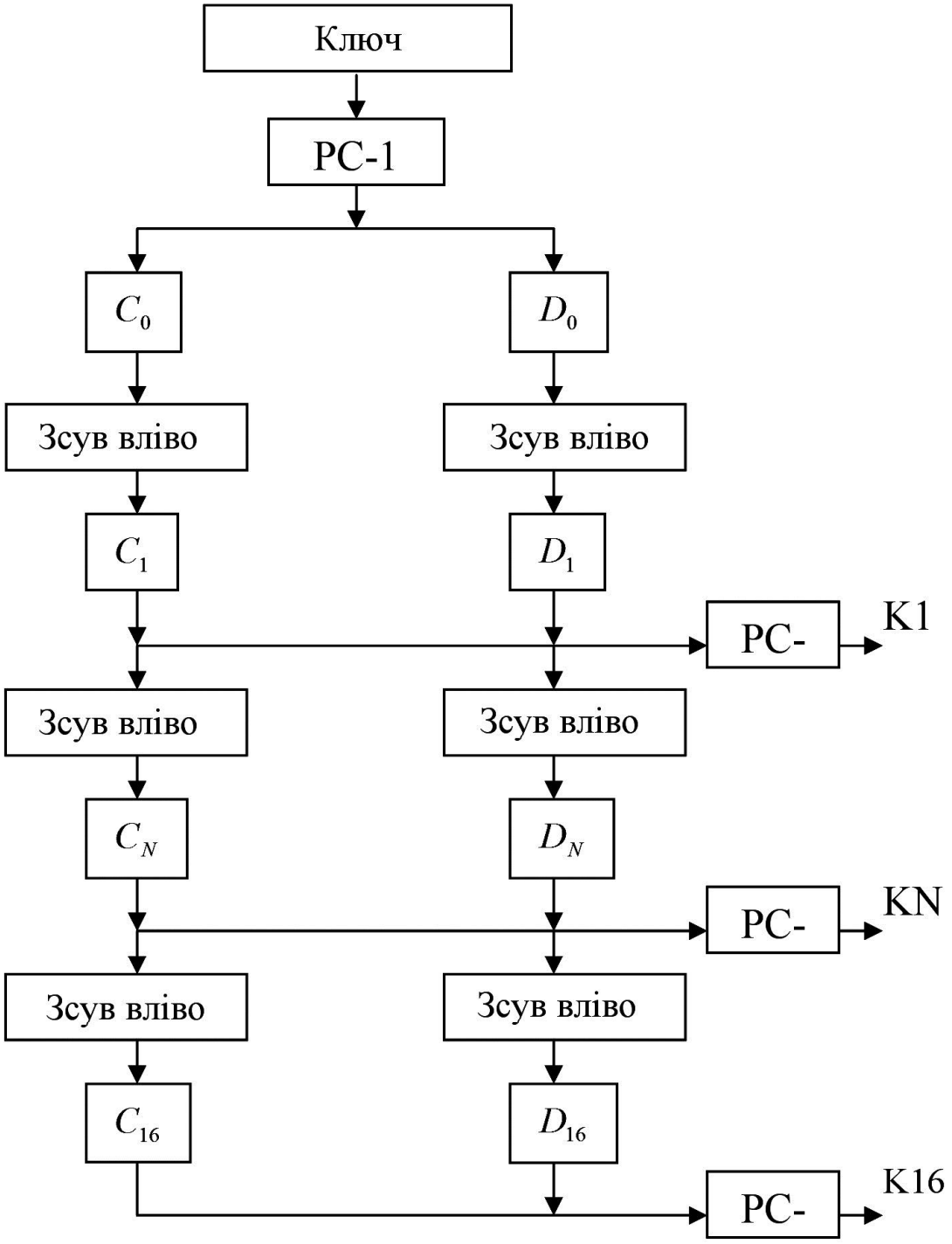

Рисунок 1.7 Алгоритм обчислення ключових блоків

Після визначення C0 і D0, ми тепер визначаємо блоки Cn і Dn, що виходять із блоків Cn-1 і Dn-1, відповідно, для n = 1, 2,..., 16. Це виконується зсувом блоків вліво дотримуючи правил з табл..1.7.

Таблиця 1.7 Розклад зсувів

№ повторювача	Число сзувів
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Наприклад, C3 і D3 виходять з C2 і D2, відповідно, двома зсівами вліво, і C16 і D16 виходять з C15 і D15, відповідно, одним зрушенням вліво. Перестановки PC-2 визначаться табл..1.8.

Таблиця 1.8 Додаткові перестановки PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Отже, перший біт Kn - це 14-й біт CnDn, другий біт - 17, і так далі з 47-й - 29-й, і 48-й біт - 32.

Отримана на виході останнього (16-го) повторювача (рис.1.5) попередня вихідна послідовність піддається перестановкам, інверсним початкової і заданим табл.1.9.

Таблиця 1.9 Перестановки інверсні початковим (IP-1)

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

При дешифруванні використовується той же самий алгоритм рис.1.5 і ключ, що і при шифруванні. Однак необхідно використовувати зворотний порядок подачі на повторювачі ключових блоків. На перший повторювач подається 16-й ключовий блок (К16), на другий-15(К15) і так далі.

1.3 Розробка технічних вимог до системи взаємодії з периферійними пристроями при обробці даних у системі DES

Основні вимоги, які пред'являються до системи крипто-охорони в стандарті DES [6]:

- забезпечувати високий рівень таємності й у той же час недвозначність і зрозумілість;
- забезпечувати для алгоритму шифрування можливість публічного використання і відкритого існування;
- при цьому необхідно домагатися такого положення, при якому тільки ключ шифру повинний бути секретним, що забезпечить універсальність у використанні алгоритму шифрування;
- запобігти можливість для конкурентів перехоплювати дані, чи заміняти видозмінювати їх без розкриття.

При виконанні цих вимог необхідно надати можливість санкціонованим користувачам одержати дані з мінімальними вартісними і тимчасовими витратами.

Особливі вимоги пред’являються до керування формуванням і розподілом ключів: ключі формуються за допомогою обов’язкових правил. Ключі повинні бути обрані випадковим образом із усіх можливих по стандарті DES 2^56 (72 квадрильйони) ключів. Ключі можна утворювати, використовуючи для цей алгоритм стандарту шифрування даних. Кожен обраний ключ повинний бути незалежний від раніше використаного ключа. Ключі можуть розподіляться і доставлятися кур’єром (вручну) чи через закриту пошту причому повинна бути виключена можливість розкрадання чи запису ключів, що доставляються. Ключі можуть розподіляться електронним способом від центра керування і розподілу ключів. У цьому випадку вони повинні зашифровуватися "головним ключем" чи "єдиним резервним ключем".

Обов’язково повинні бути прийняті надійні міри для охорони ключів:

- вони повинні бути захищені від усіх потенційних погроз їхнього розкриття;
- вони повинні бути знищені, якщо довгий час не будуть потрібні;
- при необхідності ключі повинні бути легко доступні;
- вони повинні зберігатися в пристроях, що реалізують алгоритм стандарту засекречування даних і повинні бути захищені від сторонніх облич.

У випадку, якщо ключі були скомпрометовані, чи мається якась можливість їхньої компрометації, те необхідно змінити робочі ключі. Ключі повинні бути доступні тим обличчям, що чи знають мають дані, що вони захищають.

Варто пам’ятати, що ключі можуть бути викрадені із системи, а це приведе до утрати великої кількості інформації і до тривалого порушення штатного (нормального) функціонування системи.

У стандарті DES пропонуються деякі протоколи зв’язку.

Для аутентифікації користувача можна використовувати алгоритм односпрямованого (необоротного) перетворення, при якому код аутентифікації користувача, ніколи не може бути обчислений на підставі його еквівалента, поміщеного в пам’ять машини.

Двостороння аутентифікація між терміналом і комп’ютером виробляється в тому випадку, коли єдиний ключ шифрування мається тільки в апаратурі шифрування (дешифрування) термінала і комп’ютера.

Поточні повідомленя можна шифрувально охоронити шляхом обчислення шифрувальної функції від усіх знаків повідомлення і передачі цього результату (код аутентифікації повідомлень) разом з повідомленням.

Приймач повідомлень обчислює ідентичну шифрувальну функцію прийнятого повідомлення, використовуючи такий же секретний ключ, як ключ відправника, і порівнює її з кодом аутентифікації отриманого повідомлення.

Несанкціоноване введення чи стирання повідомлень запобігається чи виявляється включенням у повідомлення якого-небудь оригінального чи унікального числа (імітотовставка).

Помилки, введені випадково чи навмисно в передані дані, можна автоматично знайти чи виправити шляхом застосування коду, що виявляє чи виправляє помилки, що міститься наприкінці переданого повідомлення і також утвориться шифрувальними методами.

Обман, типовим варіантом якого є заміна частини одного повідомлення, фрагментом з іншого повідомлення, можна запобігти, використовуючи методи аутентифікації.

Апаратура шифрування повинна встановлюватися у вихідний чи початковий стан із ключем і початковим заповненням, якщо застосовується режим шифрування зі зворотним зв’язком. Вільні місця в повідомленні повинні бути заповнені випадковими числами для того, щоб повідомлення утворювало послідовність, кратним 64 биткам. Апаратуру засекречування необхідно засинхронізувати, щоб вхід приймача з’єднувався з виходом передавача.

В апаратурі зв’язку повинні використовуватися ідентичні формати даних, а також режими шифрування, якщо такі зустрінуться. Чи виявляти виправляти помилки випливає як усередині, так і зовні закритих каналів зв’язку.

У пристроях для забезпечення конфіденційності мовних переговорів немає необхідності виконувати деякі з вимог стандарту DES. Визначається це специфікою мовного зв’язку. Користувачі пізнають (аутентифікують) один

одного по голосу, навмисне введення помилкового повідомлення (навіть раніше записаного з того ж голосу) легко виявляється по зміні змісту.

1.4 Технічні вимоги пропоновані до системи взаємодії периферійних пристроїв при обробці даних у стандарті DES

- система взаємодії з периферійними пристроями повинна працювати в режимі відкритої і закритої передачі;
- у відкритому режимі на передачі інформація не шифрується, відповідно на прийомі не дешифрується;
- відкритий режим необхідний для того, щоб можна було домовитися про номер ключа і перехід у закритий режим передачі, а також для передачі не конфіденційної інформації;
- вибір ключа будемо здійснювати комбінацією на DI- перемикачах, підключених до старших розрядів шини адреси ПЗУ;
- процесор повинний постійно аналізувати активність прийому до послідовний порт, і, якщо в нього в плині деякого часу не надходить сигнал заданого формату, то запалюється світлодіод "Втрата вхідного сигналу";
- при переході в закритий режим процесор уводить установлений DIP-перемикачам ключ і продовжує аналізувати активність прийому, якщо прийом до послідовний порт не відбувається, процесор передає в послідовний порт замість сигналу нулі і мигає світлодідом "Втрата вхідного сигналу";
- у паузах мови (якщо всі 64 біта дорівнюють нулю) у послідовний порт будемо передавати нулі (без шифрування), і, відповідно, на прийомі не дешифрувати.

1.5. Висновки до розділу

Розглянуто основні шляхи витоку інформації через технічні засоби, а також методи скремблювання і шифрування.

Варто пам’ятати, що ключі можуть бути викрадені із системи, що приведе до утрати великої кількості інформації і до тривалого порушення штатного функціонування системи

В апаратурі зв’язку повинні використовуватися ідентичні формати даних, а також режими шифрування, якщо такі зустрінуться.

У пристроях для забезпечення конфіденційності переговорів з використанням мобільних мереж немає необхідності виконувати деякі з вимог стандарту DES. Визначається це специфікою мовного зв’язку. Користувачі пізнають один одного по голосу, навмисне введення помилкового повідомлення (навіть раніше записаного з того ж голосу) легко виявляється по зміні змісту.

2 ПРИСТРІЙ ОБРОБКИ МОВНИХ ПОВІДОМЛЕНЬ

2.1 Розробка функціональної схеми системи взаємодії з периферійними пристроями

Функціональна схема системи крипто-охорони в стандарті DES приведена на рис.2.1.

Система працює в режимі відкритої й у режимі закритої передачі [2].

Вхідний сигнал через електронний трансформатор (ЕТ) надходить на аналогово-цифровий перетворювач. Електронний трансформатор служить для узгодження вхідного сигналу з АЦП по опору. В аналогово-цифровому перетворювачі сигнал відцифровується і надходить у порт Р2. Програма відправляє черговий звіт у буфер збереження даних підлягаючих шифруванню, а з буфера збереження зашифрованих даних, також черговий звіт - у послідовний порт.

У закритому режимі після прийому восьми звітів відбувається шифрування, після чого зашифровані дані надходять у відповідний буфер .

У відкритому режимі після прийому 8-ми звітів (64 біт) вони направляються в буфер збереження зашифрованих даних без шифрування. Аналогічний процес відбувається при передачі сигналу в зворотному напрямку.

Процесор постійно аналізує активність прийому до послідовного порту, і, якщо в нього не надходить у плині деякого часу сигналу заданого формату, то запалюється світлодіод "втрата вхідного сигналу", а в послідовний порт передає замість сигналу нулі.

При переході в закритий режим процесор уводить встановлений DIP-перемикачами ключ, і, якщо прийом до послідовний порт не відбувається, мигає світлодіод "втрата вхідного сигналу" [7].

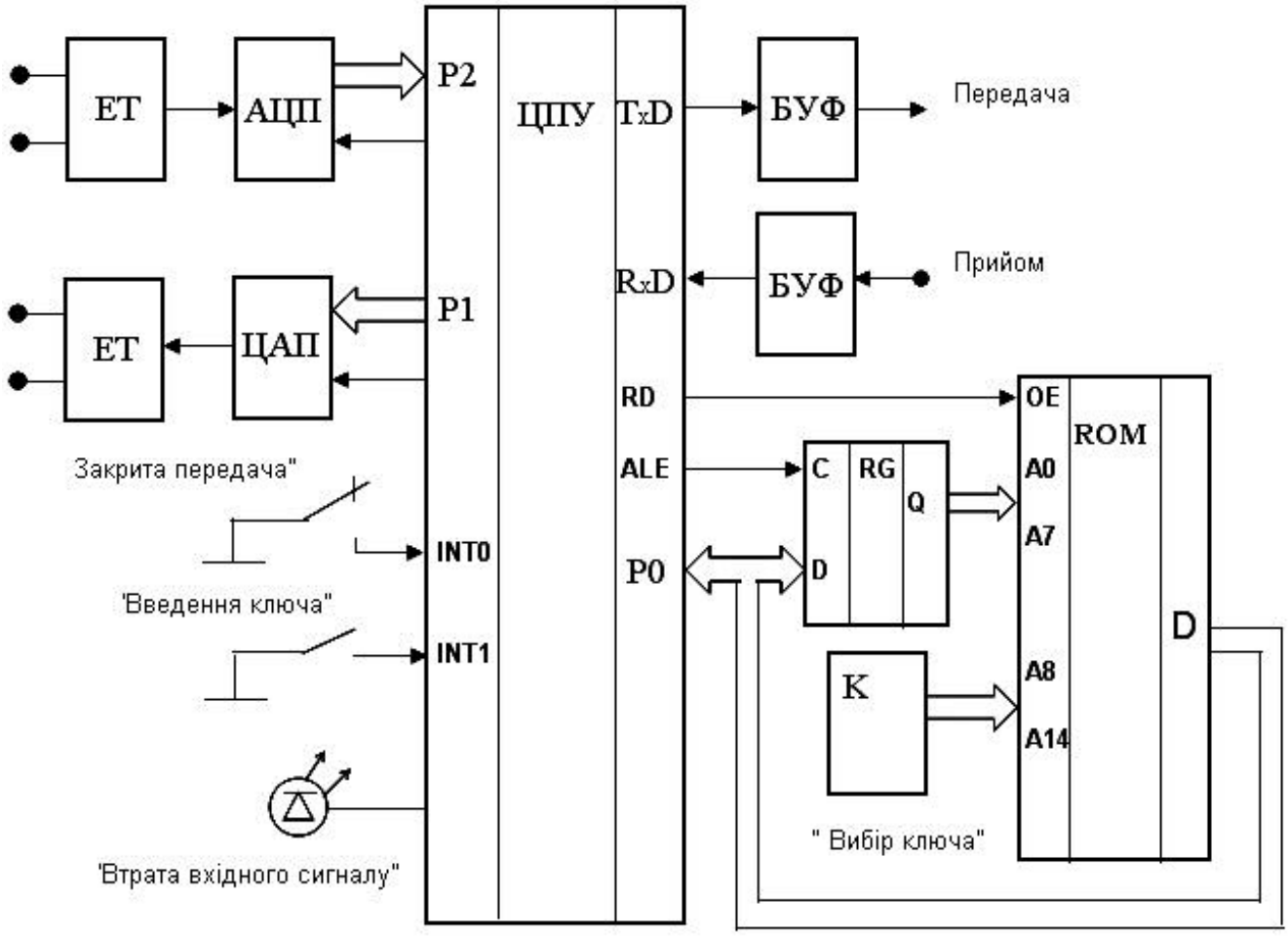

Рисунок 2.1 Функціональна схема

2.2 Розробка електричної схеми системи взаємодії з периферійними пристроями

2.2.1 Вибір елементної бази

1) Мікропроцесор

У пристрої крипто-охорони інформації в стандарті DES будемо використовувати однокристальну мікро ЕОМ сімейства МК51(MCS51) - DS87C520 фірми Dallas Semiconductor, що має наступні характеристики:

Об'єм резидентної пам’яті програм, Кбайт	16
Тип резидентної пам’яті програм	ПЗУ
Об'єм резидентної пам’яті даних, байт	256

Максимальна частота проходження тактових сигналів, МГц	55
Напруга живлення, В	5
Струм споживання, мА	8
Об'єм зовнішньої пам’яті програм, яка адресується, Кбайт	64
Об'єм зовнішньої пам’яті даних, яка адресується, Кбайт	64

Структурна організація ОМЕВМ MCS51 показана на рис. 2.2.

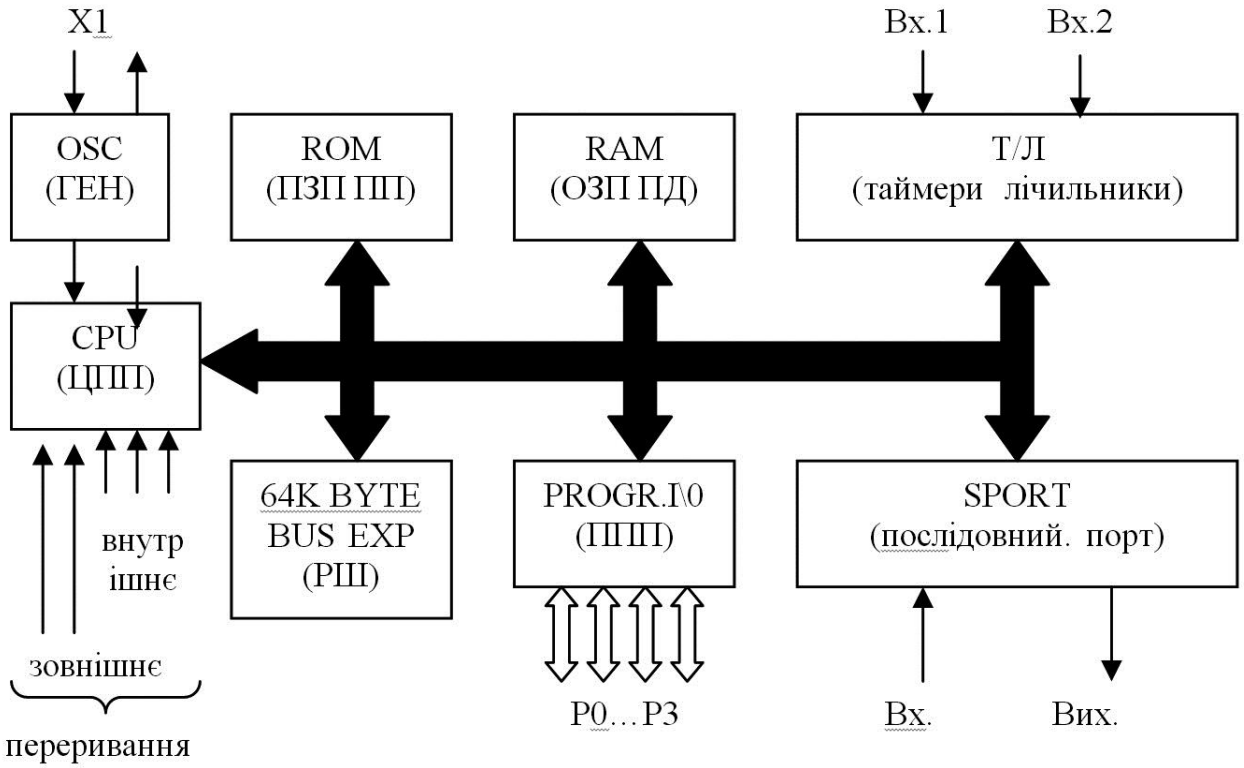

Рисунок 2.2 Структурна схема ОМЕВМ MCS51

До складу структурної схеми входять наступні функціональні вузли:

- ЦПП - центральний процесорний пристрій;
- ПЗП ПП - постійне запам’ятовуючий пристрій пам’яті програми;
- ОЗП ПД - оперативне запам’ятовуючий пристрій пам’яті даних;
- ГЕН - задаючий генератор;
- ППП - програмувальні паралельні порти;
- Послід. П - послідовний порт;
- Т/Л - таймери/лічильники;

- РШ - розширник шини для роботи з зовнішніми ЗП ємністю до 64 Кбайт.

Мікроконтролери DS87C520, оснащені EPROM пам’яттю, входять у сімейство швидкодіючих, сумісних з архітектурою 8051, мікроконтролерів фірми Dallas. Відмінною рисою цих 8-розрядних мікроконтролерів є перероблене ядро, що виключає непродуктивні такти і цикли пам’яті. У результаті ці мікроконтролери виконують кожну операцію системи команд 8051 у 1,5 - 3 рази швидше, ніж стандартний мікроконтролер 8051 , що працює на тій же тактовій частоті. Основною перевагою використання мікроконтролерів DS87C520 є підвищення швидкодії в 2, 5 рази при використанні тих же кодів і такого ж кварцового кристала. Максимальна тактова частота мікроконтролерів DS87C520 дорівнює 33 МГЦ, і їхня продуктивність еквівалентна продуктивності мікроконтролера 8051, що працює з тактовою частотою 82,5 МГЦ (приблизно в 2,5 рази вище) [8,9].

Мікроконтролери DS87C520 сумісні по висновках із усіма трьома типами корпусів стандартних мікроконтролерів 8051 і мають у своєму розпорядженні стандартні ресурси: трьома таймерами/лічильниками, послідовним портом і чотирма 8-розрядними портами I/O. Прилади оснащені 16 Кбайтами EPROM і додатковими 1 Кбайтом RAM даних. Виробляються версії як з однократним програмуванням, так і з ультрафіолетовим стиранням.

Особливістю мікроконтролерів DS87C520, крім високої швидкодії, є другий цілком апаратний послідовний порт, сім додаткових переривань, програмувальний сторожовий таймер, монітор короткочасного зниження напруги і скидання по втраті живлення. Мікроконтролер має у своєму розпорядженні здвоєний покажчик даних, що сприяють прискоренню переміщення блоків даних. Користувач може динамічно набудовувати швидкість звертання до зовнішніх пристроїв у діапазоні від 2 до 9 машинних циклів, що забезпечує необхідну гнучкість взаємодії з зовнішньою пам’яттю і периферією.

Режим керування живленням (Power Management Mode - PMM) орієнтований на використання в критичних до споживання застосуваннях - портативній апаратурі й апаратурі з батарейним живленням. Ця функція

дозволяє програмно встановлювати, у якості основної тимчасової бази, більш низьку тактову частоту. І якщо в нормальному режимі тривалість машинного циклу складає 4 такти, то режим РММ дозволяє процесору виконувати машинний цикл за 64 чи 1024 такту. Наприклад, при тактовій частоті 12 МГц частота виконання машинних циклів складає 3 Мгц. У режимі РММ програма може установити частоту машинних циклів187,5 чи 11,7 кГц. Таке зниження частоти приводить, відповідно, до зниження споживання процесора за рахунок його більш повільної роботи.

Мікроконтролер DS87C520 має у своєму розпорядженні функцію, що істотно знижує рівень електромагнітних випромінювань. Ця функція дозволяє програмно встановлювати заборону на формування сигналу ALE, у тих випадках, коли в ньому немає необхідності.

Система переривань ОМЕВМ DS87C520 підтримує переривання від п’яти джерел:

INT0- зовнішнє переривання по стані/ зміні стану логічного сигналу на вході INT0 (вивід 12).

INT1-зовнішнє переривання по стані/зміні стану логічного сигналу на вході INT1 (вивід 13).

T/C0- внутрішнє переривання по переповненню таймера/лічильника Т/З0.

T/C1- внутрішнє переривання по переповненню таймера/лічильника Т/З0.

S- внутрішнє переривання від послідовного порту.

Переривання в загальному виді є засобом змусити процесор припинити виконання поточної програми і перейти до виконання іншої програми (підпрограми), що є частиною загального для розв’язуваної задачі прикладного програмного забезпечення, і асоційованої з даним перериванням.

Кожним джерелом може бути сформований запит на переривання, що установлює відповідний прапор, обслуговування запитів може бути дозволене чи заборонено.

Кожному з джерел переривань може бути установлений високий чи низький пріоритет установкою/ скиданням відповідних біт у регістрі IP; при

цьому підпрограми переривань більш високого пріоритету можуть переривати підпрограми більш низького.

2) Постійний запам’ятовуючий пристрій

Для збереження комбінацій ключів використовуємо IMC M27C256B фірми STMicroelectronics. Вона являє собою постійний запам’ятовуючий пристрій. До старшого шести розрядам підключимо DiP - перемикачі для вибору ключів, що самі собою є індикаторами. Кількість ключів буде дорівнювати:

$$N = 2^7 = 128$$

3) Регістр

Тому що для звертання до зовнішнього ПЗУ і зчитування з його даних ми використовуємо одну шину, то для запам’ятовування адреси осередку використовуємо 8 бітовий регістр DM74ALS573B фірми Fairchild.

Введення ключа в процесор відбувається в такий спосіб:

При звертанні до зовнішньої пам’яті на P0 з’являється адреса осередку по який у ПЗУ зберігається комбінація ключа, після установки сигналу ALE ця адреса запам’ятовується регістром і з’являється на адресній шині (молодший байт) мікросхеми пам’яті. Після появи сигналу RD з порту P0 зчитуються дані з даної адреси.

4) АЦП

Для перетворення аналогових сигналів в цифрові візьмемо 8 бітовий АЦП фірми ANALOG DEVICES AD7574, який використовує метод послідовних наближень і забезпечує швидкий час конверсії сигналу 15 мкс.

5) ЦАП

А для перетворення цифрового сигналу в аналоговий використаємо 8 бітовий ЦАП також фірми ANALOG DEVICES AD557.

6) Підсилювач

У системі крипто-охорони, такій як електронний трансформатор, застосуємо операційний підсилювач ДО140УД20А.

Операційний підсилювач - це транзисторний многокаскадний підсилювач постійного струму, виконаного у вигляді ІМС, що обумовлює його схемотехнічні особливості. Структурна схема операційного підсилювача, рис. 2.3, містить диференціальний вхідний каскад, каскади посилення і вихідний каскад, що забезпечує задану потужність сигналу в навантаженні [10, 11].

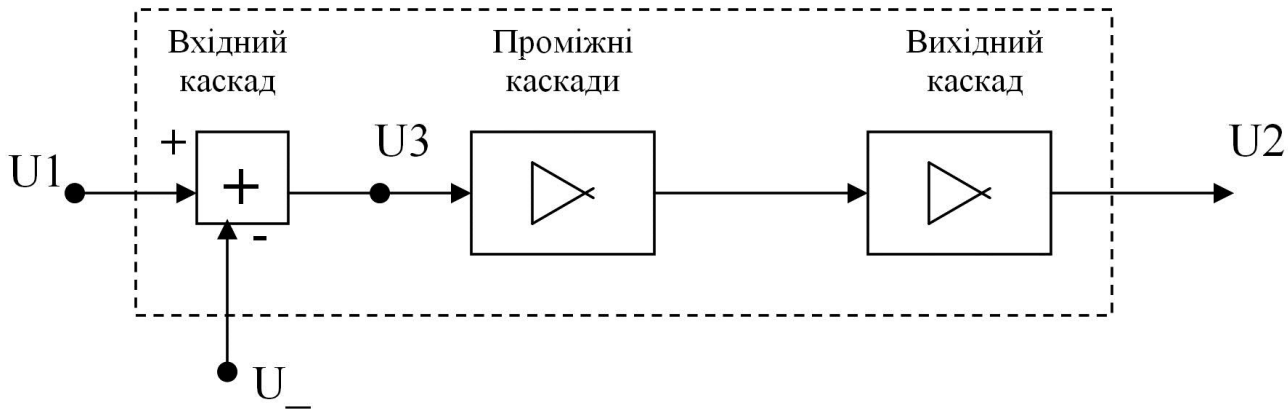

Рисунок 2.3 Структурна схема операційного підсилювача

Диференціальний вхідний каскад являє собою мостову схему з двома входами, причому на його вихід сигнал з одного входу (прямого) подається без змін фази, а з іншого входу (інверсного) - у противофазі. Стабільність робочої крапки вхідного каскаду забезпечується за рахунок глибокого негативного зворотного зв'язку, створюваної в емітерному ланцюгу, тому вхідний опір входів операційного підсилювача - дуже високе.

Основне посилення К=U2/U3 вносять проміжні каскади.

Вихідний каскад операційного підсилювача виконаний на парі комплементарних (з доповнювальними друг друга характеристиками) транзисторів, що утворять відносно різнополярних джерел живлення міст.

Двополярне електроживлення забезпечує рівність потенціалів обох входів і виходу потенціалу корпуса, тому операційний підсилювач звичайно не має потребу в ланцюгах поділу по постійному струмі.

Операційні підсилювачі завжди охоплюють глибоким рівнобіжним по виходу негативним зворотним зв’язком, з’єднуючи вихід з інверсним входом. Завдяки цьому різко поліпшуються їхня стабільність, частотні й інші характеристики, знижується до десятків ом вихідний опір. На практиці вхідний опір операційного підсилювача можна вважати нескінченним, а вихідне - нульовим. Схема операційного підсилювача, що не інвертує сигнал, приведена на рис. 2.4.

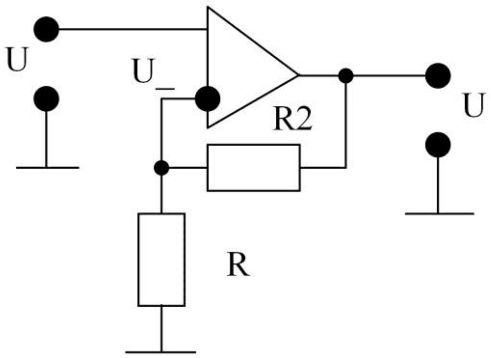

Рисунок 2.4 Схема операційного підсилювача, який не інвертує сигнал

У ланцюзі зворотного зв’язку включений дільник напруги з коефіцієнтом передачі:

$$\beta = \frac{R_1}{(R_1 + R_2)}$$

Тоді вираз для коефіцієнта підсилення не інвертує операційного підсилювача:

$$K_{OC} = \frac{1}{\beta} = 1 + \frac{R_2}{R1}$$

Коефіцієнт підсилення, у нашому випадку, дорівнює двом, тоді R1=R2=10 кому.

Для операційного підсилювача, що інвертує (рис. 2.5), коефіцієнт підсилення:

$$K_{инв} = \frac{R_2}{R1}$$

При коефіцієнті підсилення рівному одиниці R1=R2=10 кОм.

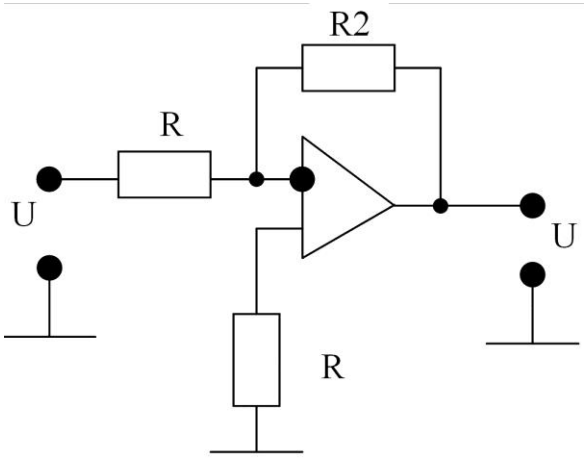

Рисунок 2.5 Схема операційного підсилювача, що інвертує

На вході операційного підсилювача, для забезпечення необхідного загасання відображення й асиметрії розрахуємо дільник (рис. 2.6) на резисторах R1,R2,Rx [12].

Загасання відображення:

$$A_{відобр} = 10\lg\left|\frac{(R1+R2)-600}{R1+R2+600}\right|$$

Необхідна $A_{відобр}$=26дб, тоді R1=R2=301 Ом.

Захищеність асиметрії:

$$A_{асим} = 20\lg\left|\frac{R1+Rx+R2+Rx}{R1+Rx-(R2+Rx)}\right|$$

Необхідна $A_{асим}$ = 52дб, тоді при допуску резисторів ±5% Rx=10 кОм.

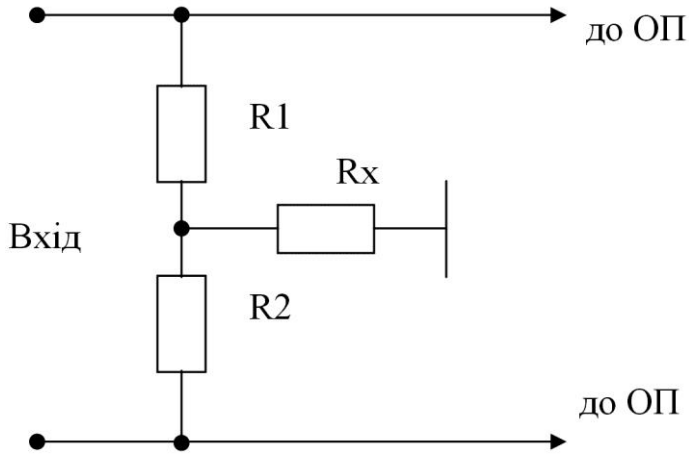

Рисунок 2.6 Погоджувальний пристрій

7) Підсилювач потужності вихідного сигналу

Для збільшення потужності сигналу на виході і вході системи, тобто збільшення високого рівня напруги, використовуємо IMC SN54LS05 фірми Texas Instruments. Ця мікросхема представляє собою 6 інверторів з відкритим колекторним виходом [13].

На рис.2.7 представлена закінчена принципова електрична схема пристрою.

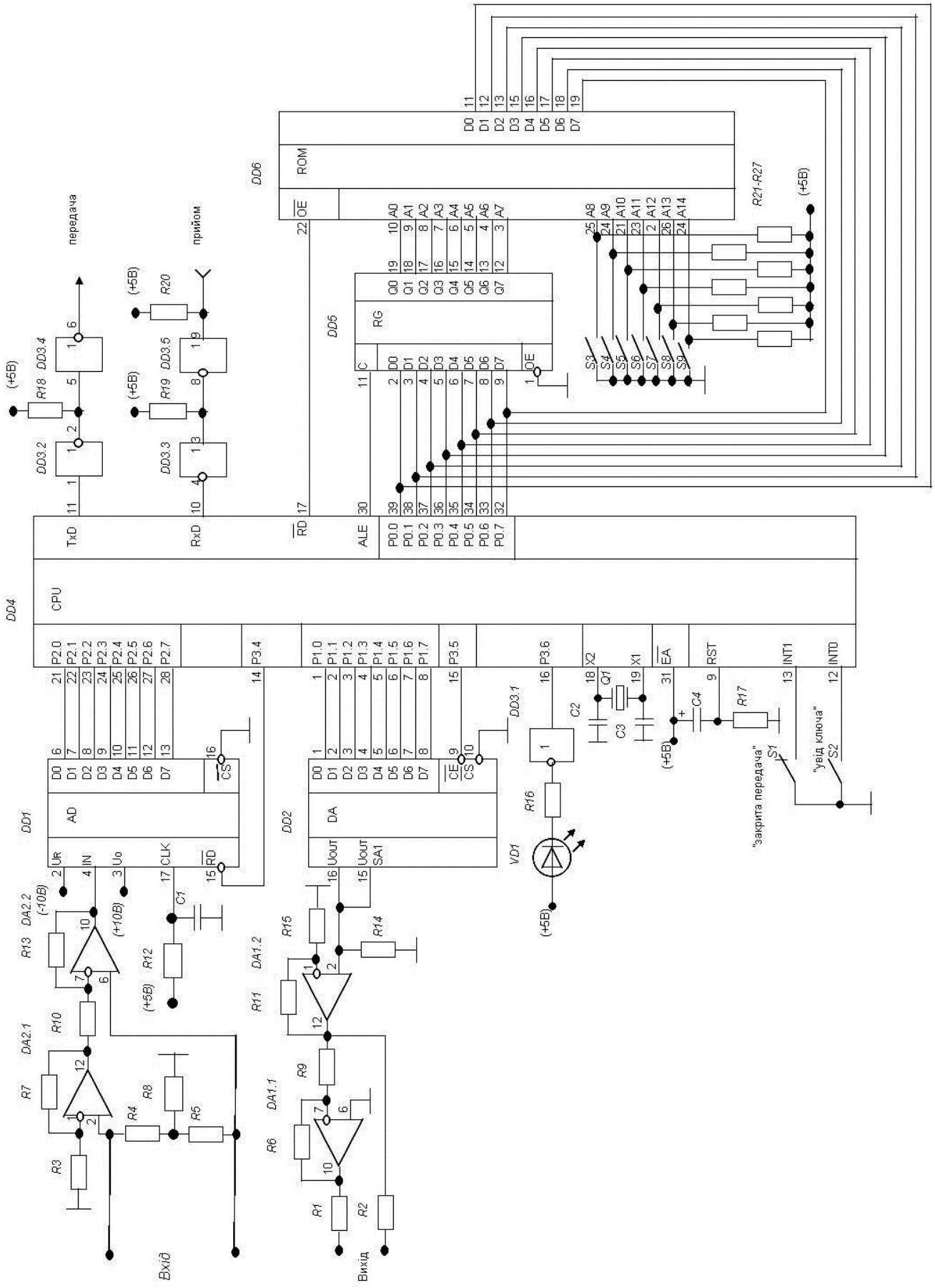

Рисунок 2.7 Електрична принципова схема системи взаємодії з периферійними пристроями

2.3 Висновки до розділу

Розроблена функціональна та принципова електрична схеми системи взаємодії з периферійними пристроями.

У пристрої крипто-охорони інформації в стандарті DES використано однокристальну мікро ЕОМ сімейства МК51(MCS51) - DS87C520 фірми Dallas Semiconductor, що має необхідні характеристики. Для збереження комбінацій ключів використано IMC M27C256B фірми STMicroelectronics. Режим керування живленням орієнтований на використання в критичних до споживання застосуваннях - портативній апаратурі й апаратурі з батарейним живленням.

3 РОЗРОБКА АЛГОРИТМІВ І ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ВЗАЄМОДІЇ З ПЕРЕФЕРІЙНИМИ ПРИСТРОЯМИ

На рис.3.1 представлена блок-схема алгоритму системи взаємодії периферійних пристроїв з урахуванням технічних вимог розроблених раніше, а на рис.3.2 - рис.3.5 алгоритми програми переривань: INT0, INT1, Т/Л0, S.

У нашому пристрої будемо використовувати переривання в наступних цілях:

INT0 (низький пріоритет, рівневий режим переривань)- для переходу в режим закритої передачі і назад.

INT1(низький пріоритет, крайовий режим переривань)- для введення ключа.

Т/Л0(високий пріоритет)- для формування сигналів керування АЦП із f=64/8=8кгц, Т=125мкс(період повторення).

Для одержання необхідної частоти визначимо перезавантажувальне число, що міститься в регістрі ТН0:

Період машинного циклу при частоті генератора, що задає, 55 МГЦ:

$$T_{Ц} = \frac{4}{f_T} = \frac{4}{55 \cdot 10^6} = 72 \cdot 10^{-9}$$

Перезавантажувальне число дорівнює:

$$n = 256 - \frac{T_{ПОВТ}}{T_{Ц}} = 256 - 173 = 83$$

S (високий пріоритет) - використовуємо для зчитування звіту надійшовшого в послідовний порт.

Швидкість передачі визначається частотою переповнення Т/Л1, що працює в режимі 2. Швидкість передачі описана виразом:

$$f = (\frac{2^{SMOD}}{32})(\frac{f_{РЕЗ}}{4})(256 - (TH1))$$

При швидкості передачі 115200 біт/зі знайдемо ТН1:

ТН1=255

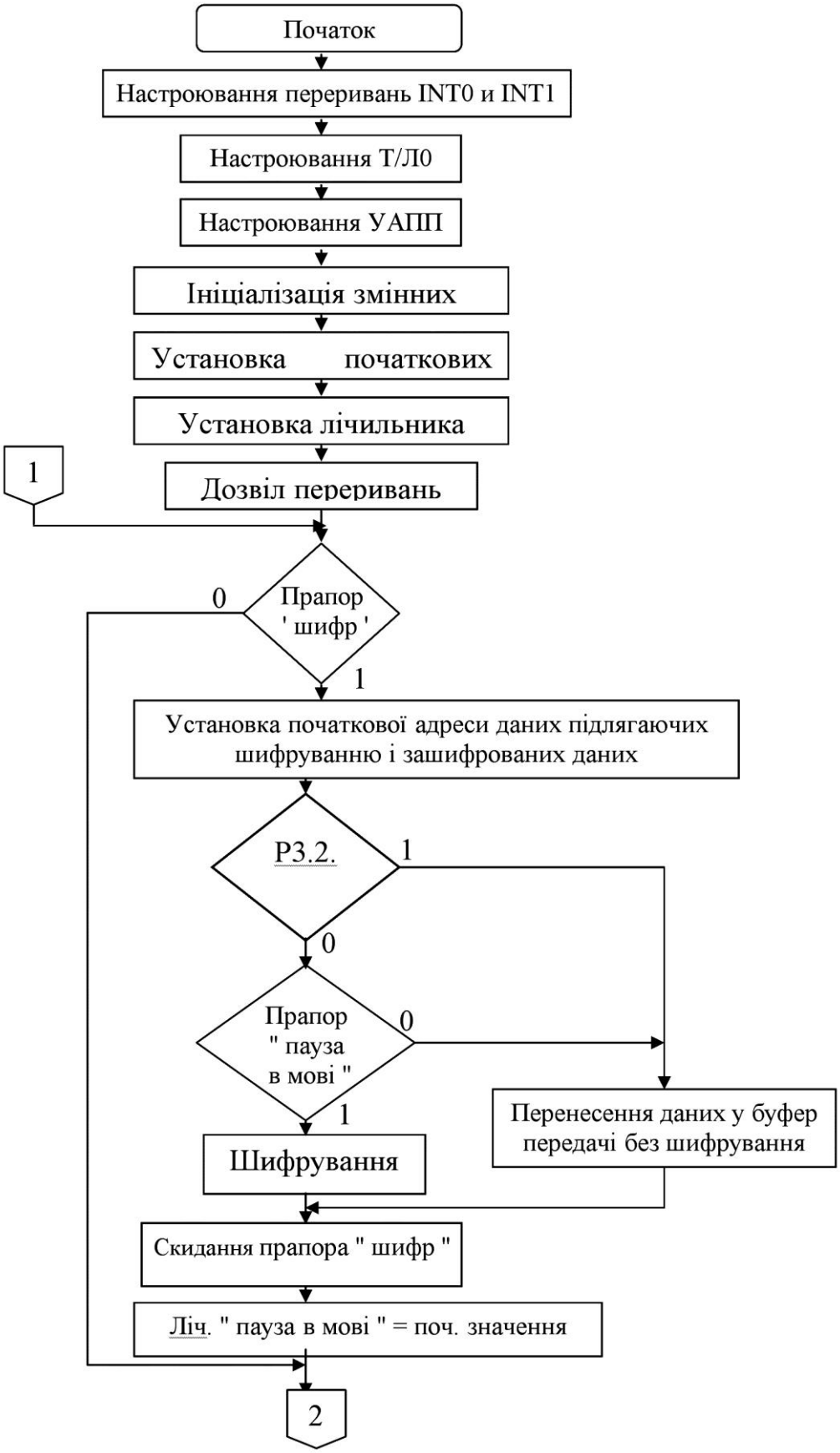

Рисунок 3.1 Алгоритм роботи системи взаємодії з периферійними пристроями (початок)

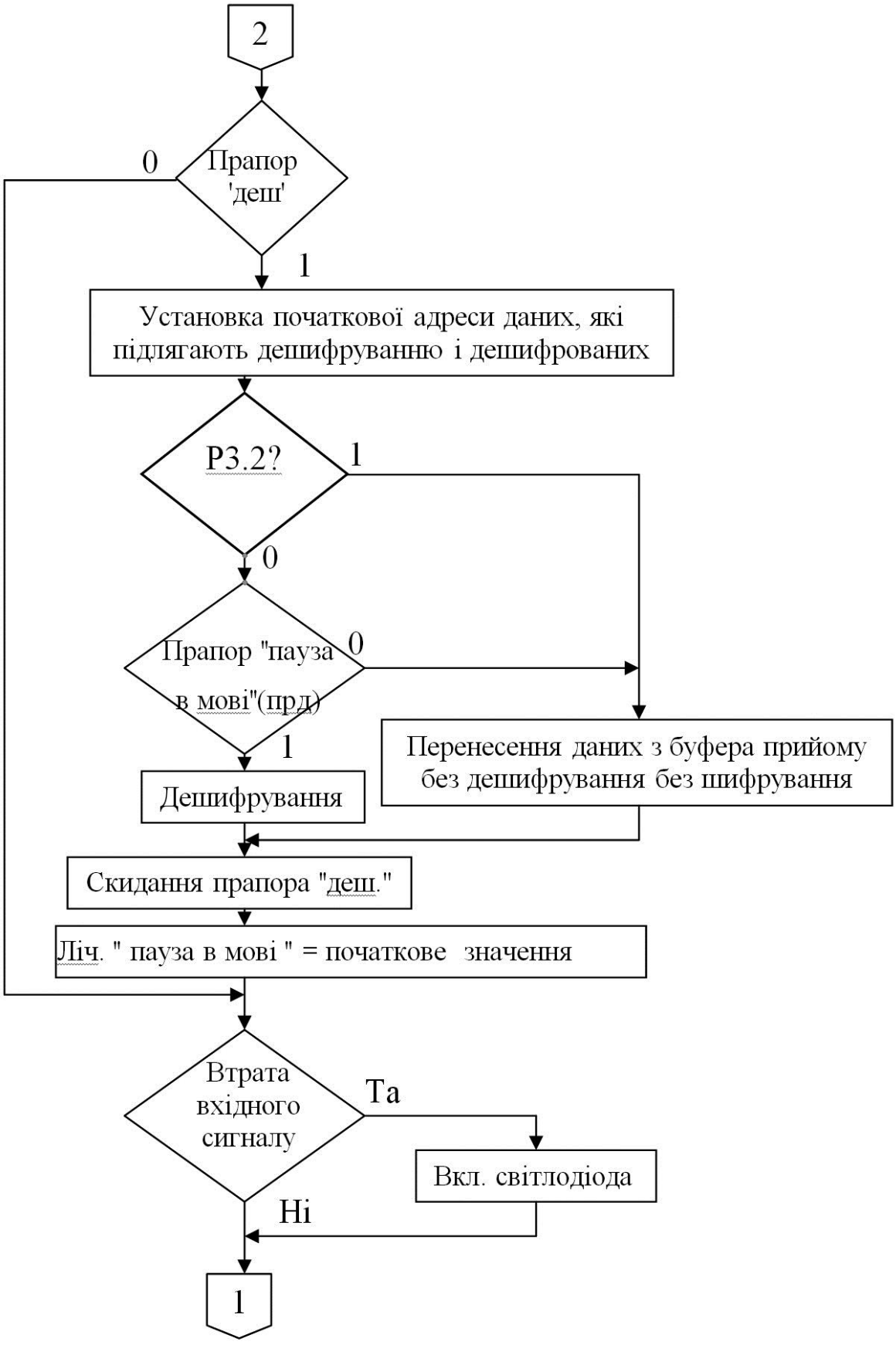

Рисунок 3.1 Алгоритм роботи системи взаємодії з периферійними пристроями (закінчення).

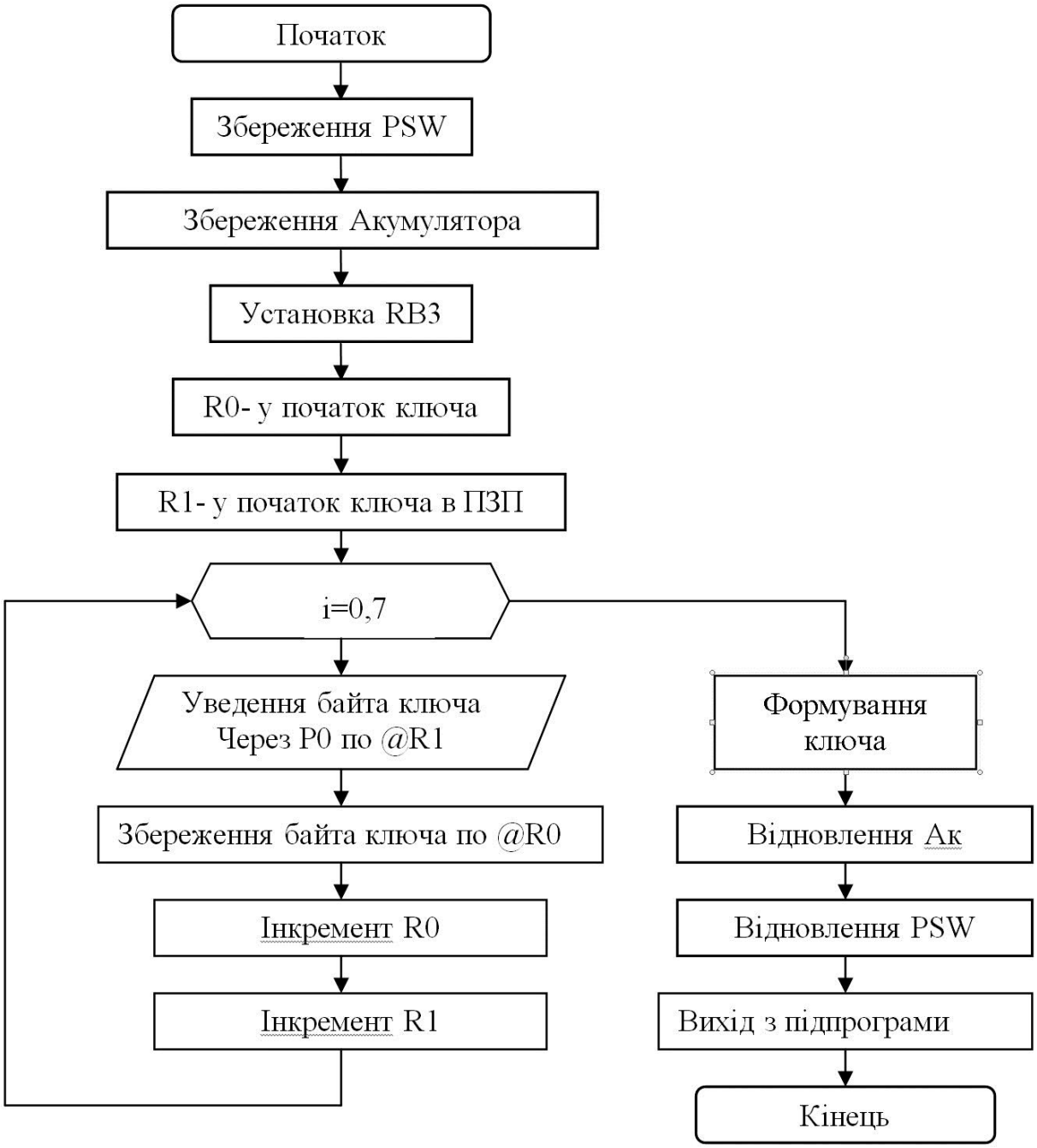

Рисунок 3.2 Підпрограма обробки переривань від INT1(низький пріоритет)

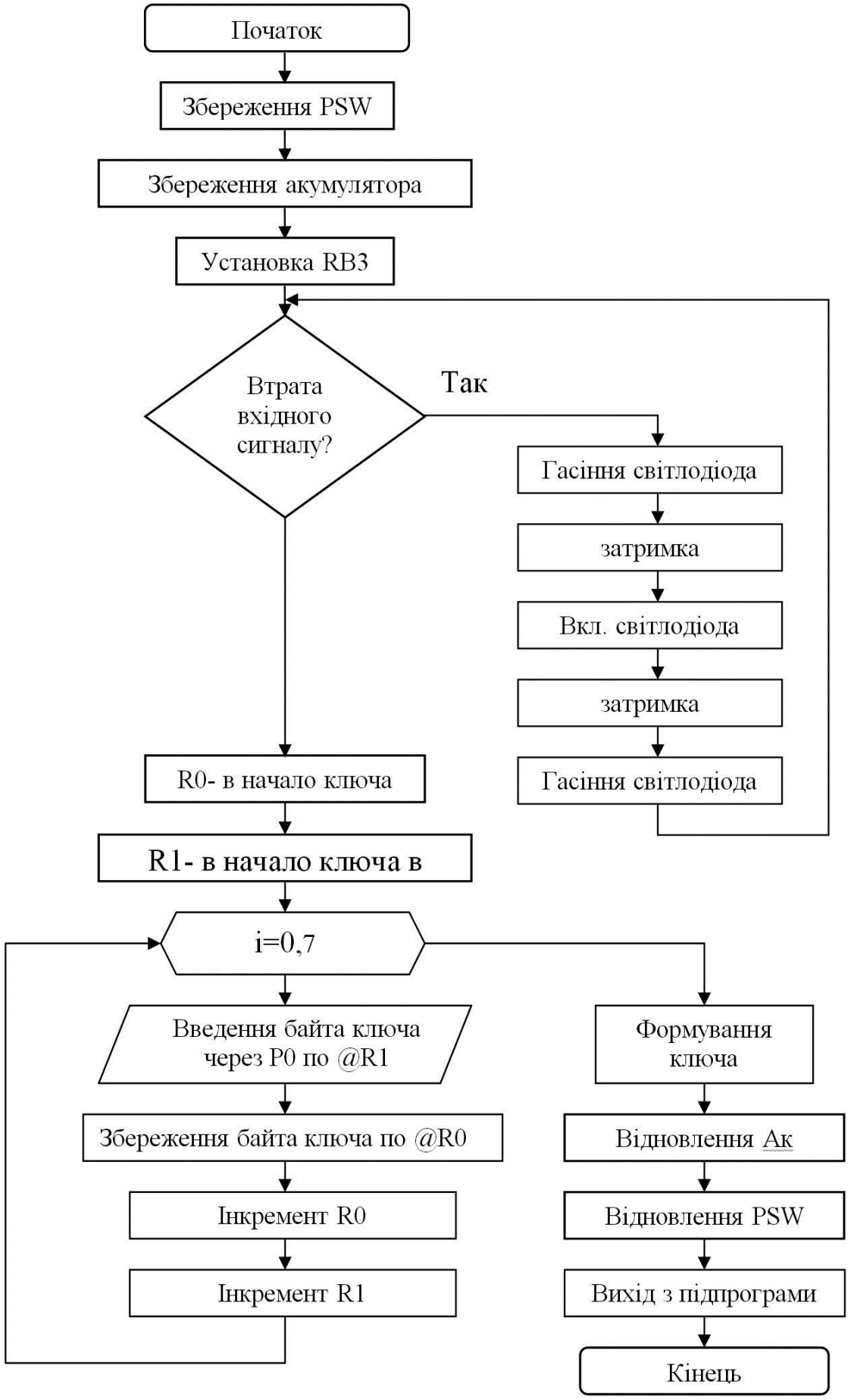

Рисунок 3.3 Підпрограма обробки переривань від INT0 (низький пріоритет)

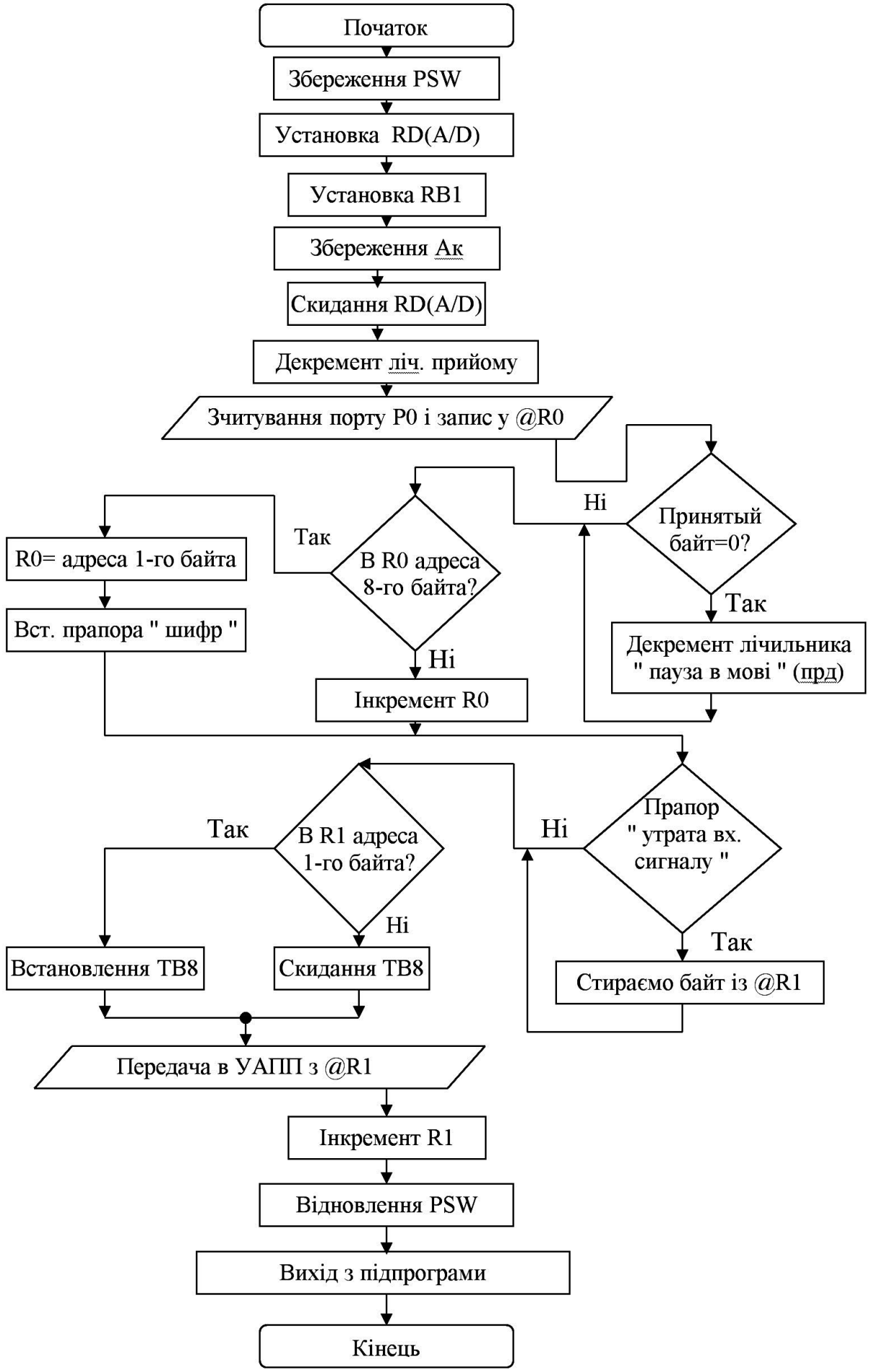

Рисунок 3.4 Підпрограма обробки переривань від Т/Л0 (високий пріоритет)

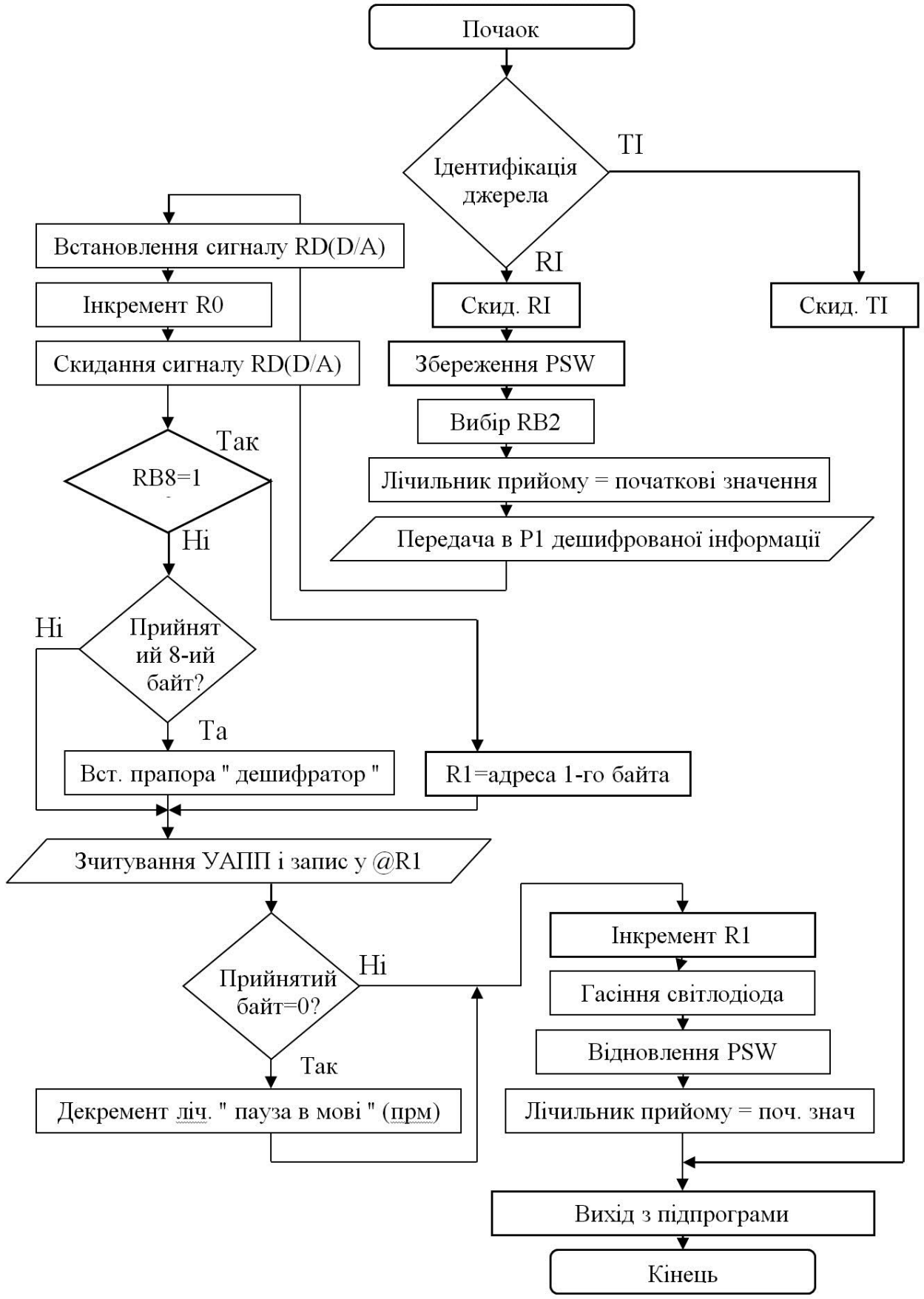

Рисунок 3.5 Підпрограма обробки переривань від УАПП (високий пріоритет)

ВИСНОВКИ

Розвиток мікроелектроніки і широке застосування її виробів у промисловому виробництві, у пристроях і системах керування найрізноманітнішими об’єктами і процесами є в даний час одним з основних напрямків науково-технічного прогресу.

Використання мікроелектронних засобів у виробах виробничого і культурно-побутового призначення не тільки приводить до підвищення техніко-економічних показників (вартості, надійності, споживаній потужності, габаритних розмірів) і дозволяє багаторазово скоротити терміни розробки і відсунути терміни "морального старіння" виробів, але і додає їм принципово нові споживчі якості (розширені функціональні можливості, модифицируемость, адаптивність і т.д).

Використання мікроконтролерів у системах керування забезпечує досягнення виняткове високих показників ефективності при настільки низької вартості (у багатьох застосуваннях система може складатися тільки з один БІС мікроконтролера), що мікроконтролерам, видимо, немає розумної альтернативної елементної бази для побудови керуючих і/чи регулюючих систем. До дійсного часу більш двох/третин світового ринку мікропроцесорних засобів складають саме однокристальні мікроконтролери.

В даний час випускається численні однокристальні мікроевм, орієнтовані на використання в телекомунікаційних системах – трансиверах цифрових потоків E1 і T1, інтегральні пристрої стиску мовної інформації, процесори голосової пошти, автовідповідачі, тональні приймачі/генератори і т.п.

Використовувавши в данній бакалаврській роботі однокристальну мікро-ЕОМ нам вдалося реалізувати в досить компактному пристрої винятково складний алгоритм, що вимагає для своєї реалізації десятки тисяч електронних елементів, об’єднаних у сотні регістрів і схем. Застосування малогабаритної цифрової пам’яті з великими термінами збереження й обсягами збереженої інформації дозволяє постачати пристрій взапас великою кількістю ключів.

Розроблений пристрій крипто-охорони засновано на використанні алгоритму шифрування DES, що дозволяє робити обмін інформації при використанні з пристроями інших фірм з аналогічним алгоритмом шифрування.

При використанні пристрою крипто-охорони в стандарті DES, оператор повинний знати що, теоретично, при підборі ключів супротивник може його знайти без використання всіх комбінацій. Тому потрібно вживати заходів для охорони ключів.

Стійкість алгоритму DES може бути підвищена за допомогою визначених удосконалень і модифікацій. Створювані на основі стандарту DES пристрої повинні розроблятися так, щоб їх можна було використовувати в обчислювальних чи системах мережах для забезпечення шифрувальної охорони даних, представлених у виді двійкового коду. При цьому повинна бути забезпечена можливість їхніх іспитів і перевірки на точне виконання перетворень.

ПЕРЕЛІК ВИКОРИСТАНОЇ НАУКОВО-ТЕХНІЧНОЇ ЛІТЕРАТУРИ

1. Калинцев Ю.К. Конфиденциальность и защита информации. –М.: МТУСИ, 1997.
2. Сударев И.В. Криптографическая защита телефонних сообщений // Специальная техника.
3. Дворянкин С.В., Девочкин Д.В. Методи закрития речевих сигналов в телефонних каналах // Конфидент, 1995, № 5.
4. Лагутин В.С., Петраков А.В. Утечка и защита информации в телефонних каналах. – М.: Енергоатомиздат, 1996.
5. FIPS PUB 46 (Федеральная информационная служба по стандартам, публикация 46. “Описание стандарта DES для засекречивания данних”).
6. Сташин В.В. и др. Проектирование цифрових устройств на однокристальних микроконтроллерах / В.В. Сташин, А.В. Урусов, О.Ф. Мологонцева. – М.:Енергоатомиздат, 1990.
7. http://st.ess.ru/publications/articles/analit/newtech.htm
8. http://www.phreaking.ru/showpage.php?pageid=53351
9. http://www.kvirin.com/stat/sb4.htm
10. http://www.cnews.ru/newcom/index.shtml?2004/12/15/170303
11. http://securit index.php?mode=articles&id=204ystar.ru/
12. http://www.author.kiev.ua/index.php?page=vdcrypt
13. Методические указания по дисциплине “Техника микропроцессорных систем в электросвязи”. – М.: МТУСИ, 1998.

ДОДАТКИ

Додаток А : Правила запису програми на мові асемблер

Додаток А

Правила запису програми на мові асемблер

При складанні програми розробник зазвичай користується мовою більш високого рівня, ніж мова машинних команд (зазвичай використовується мова асемблера даного процесора або більш універсальна мова С), при цьому текст програми перекладається в необхідну для пристрою, що запам'ятовує пам'яті програм сукупність двійкових символів за допомогою ЕОМ з використанням спеціальних програм, які отримали назву трансляторів. Програма-транслятор, що базується на мнемокодах системи команд якогось конкретного процесора, зазвичай називається асемблером даного процесора.

При складанні програми на мові асемблера слід мати на увазі ряд правил, дуже схожих, проте мають відмінності для конкретних ассемблеров. Нижче наведено звід правил складання програм на мові асемблера.

Програма записується у вигляді послідовності операторів. Кожен оператор займає один рядок програми. У тексті програми допускається використання наступних символів:

- малих і великих літер латинського алфавіту;
- цифр 0 ... 9;
- спеціальних знаків " # ", " @ ", "; ", ": ", ", ";
- знаків математичних дій.

Текст програми для кожного оператора розбивається на чотири поля-поле мітки, поле коду операції, поле операндів і поле коментарів. Заповнення полів не є обов'язковим за винятком випадку заповнення поля коду операції мнемокод команди, що вимагає вказівки операндів. Поля розміщуються в тексті в зазначеному порядку і відокремлюються одна від одної як мінімум одним пропуском або табуляцією.

Поле мітки починається з першої позиції тексту (крайнє ліве положення курсору на екрані) і містить мітку, яка може бути вказана в будь-якому місці сегмента як адреса переходу.

Якщо мітка в операторі не використовується, перша позиція тексту повинна бути вільна (містити пробіл).

Мітка являє собою будь-яку комбінацію латинських букв, цифр і символу підкреслення, що починається з букви і містить не більше семи символів. Після мітки ставиться двокрапка (без відділення прогалиною). Кожна мітка повинна мати своє унікальне ім'я, повторення міток в програмі не допускається.

Поле кодів операцій і поле операндів заповнюються Мнемокод команд процесора або Мнемокод псевдоінструкцій асемблера. Якщо в поле операндів вказані два операнда, вони розділяються між собою комою. Якщо в якості операнда вказується число, воно повинно починатися з символу #. Як числа, так і номери осередків пам'яті можуть бути представлені в різних системах числення, при цьому в кінці числа або номера осередку ставиться символ відповідної системи:

B - двійковій;

H - шестнадцатерічної.

Якщо символ приналежності до системи числення в кінці числа або номера осередку відсутня, відповідний номер або число сприймається транслятором в десятковій системі числення.

Поле коментарів повинно починатися з символу " крапка з комою ". Це поле використовується на розсуд програміста для підвищення зручності читання програми. Інформація, що міститься в поле коментарів, які не транслюється асемблером і не впливає на виконання програми процесором.

Налагодження програми.

Налагодження програмного забезпечення зручно вести за окремими частинами, які виконують конкретні закінчені функції. У нашому випадку ми маємо 5 закінчених функцій (сегментів), їх налагодження будемо робити в наступному порядку:

1. Основна програма.

2. Підпрограма обробки переривань від INT0.

3. Підпрограма обробки переривань від INT1.

4. Підпрограма обробки переривань від УАПП.

5. Підпрограма обробки переривань від Т / С0.

Процес компонування здійснимо на ЕОМ за допомогою програми-лінковщік.

Програма, написана на мові програмування асемблер, налагоджена і довела свою працездатність за допомогою пакета симуляції AVSIM51. Лістинг трансляції наведено нижче:

Програма мовою Асемблер

```
;порт Р2-введення даних від АЦП
;порт Р1-висновок на ЦАП
;у R0(RB0) адреса (38Н-3FH) даних для шифрування
;у R1 (RB2) АДРЕСА (20Н-27Н) ДАНІ ДЛЯ ДЕШИФРУВАННЯ
;у R1 (RB0) адреса (30Н-37Н) для зашифрованого повідомлення
;у R0 (RB2) адреса (28Н-2FH) для дешифрованого повідомлення
;Р3.5-СИГНАЛ ДЛЯ КЕРУВАННЯ РОБОТОЮ ЦАП
;Р3.4-СИГНАЛ ДЛЯ КЕРУВАННЯ РОБОТОЮ АЦП
;Р3.6-СВЕТОДИОД "УТРАТА ВХІДНОГО СИГНАЛУ"
;int0-  1-ВІДКРИТА ПЕРЕДАЧА, 0-ЗАКРИТА ПЕРЕДАЧА
;int1-ВВЕДЕННЯ КЛЮЧА
;40Н-47Н-яч.ЗУПД ДЛЯ ЗБЕРЕЖЕННЯ 8 байт ключа
;0Н-8Н- яч ВПЗП ДЕ ЗБЕРІГАЄТЬСЯ КЛЮЧ
;12Н-ЛІЧИЛЬНИК ПРИЙОМУ (ЯКЩО =0 ТЕ НЕМАЄ ПРИЙОМУ)
;13Н-ПРАПОР "ДЕШИФРОВНИЕ"(ЯКЩО =0 ТЕ НЕ ДЕШИФРУВАТИ)
;14Н-ПРАПОР "ШИФРУВАННЯ" (ЯКЩО =0 ТЕ НЕ ШИФРУВАТИ)
;15Н-ПРАПОР "ПАУЗА В МОВІ" НА ПЕРЕДАЧІ (ЯКЩО =0 ТЕ ПРИЙНЯТЕ 8 БАЙТ=0)
;16Н-ПРАПОР "ПАУЗА В МОВІ" НА ПРИЙОМІ
;
;
        DEFSEG          BEG,ABSOLUTE
```

```
        SEG   BEG
        ORG   0H
        AJMP  MET2
        ORG   03H
        AJMP  INTER0
        ORG   0BH
        AJMP  TIMER
        ORG   13H
        AJMP  INTER1
        ORG   023H
        AJMP  SER_P
MET2:   SETB  IT0           ;вст. КРАЙОВИЙ режим переривань INT0
        SETB  IT1           ; вст. КРАЙОВИЙ режим переривань INT1
        CLR   PX0           ; НИЗЬКИЙ ПРІОРИТЕТ INT0
        CLR   PX1           ;--\\--\\--\\--  INT1
        SETB  EX0           ; ДОЗВІЛ ПЕРЕРИВАНЬ INT0
        SETB  EX1       ;
        MOV   TMOD,#00100010B ; УСТАНОВКА Т\Л У РЕЖИМ 2
        MOV   TH1,#54       ; ПЕРЕЗАГРУЖ.ЧИСЛО ДЛЯ УСТ ШВИДКОСТІ УАПП
        MOV   TH0,#50       ; ДЛЯ ЗЧИТУВАННЯ Р2 С F=8КГЦ
        CLR   ET1           ; ЗАБОРОНА ПЕРЕР ВІД Т\Л1
        SETB  ET0           ; ДОЗВІЛ ПЕРЕР ВІД Т\Л0
        SETB  PT0           ; ВИСОКИЙ ПРІОРИТЕТ Т\Л0
        MOV   SCON,#11010000B  ;ВСТ РЕЖ 3 УАПП
        SETB  ES            ; РАЗРЕШ ПЕРЕР ВІД УАПП
        SETB  PS            ; ВИСОКИЙ ПРІОРИТЕТ УАПП
        MOV   00H,#38H      ; ВСТ ПОЧ АДРЕСИ ДАНИХ ДЛЯ ШИФРУВАННЯ
        MOV   01H,#30H      ;--\\--\\--\\--\\ ДЛЯ ЗАШИФРОВАННОГО ПОВІД.
        MOV   10H,#28H      ;---\\---\\---\\- ДЛЯ ДЕШИФР. ПОВІД.
        MOV   11H,#20H      ;---\\---\\---\\-ДАНИХ ДЛЯ ДЕШИФРУВАННЯ
        MOV   18H,#40H      ; ВСТ. АДРЕСИ ПЕРШОГО БАЙТА КЛЮЧА В CPU
        MOV   19H,#0H               ;---\\---\\---\\---\\---\\---\\--В ВПЗП
        MOV   12H,#0                ; ВСТАНОВЛЕННЯ ЛІЧИЛЬНИКА ПРИЙОМУ
        MOV   13H,#0                ; ПРАПОР ДЕШИФРУВАННЯ
        MOV   14H,#0                ; ПРАПОР ШИФРУВАННЯ
```

```
        MOV   15H,#8        ; ПРАПОР "ПАУЗА В МОВІ" НА ПЕРЕДАЧІ
        MOV   16H,#8              ;---\\---\\---\\---\\ НА ПРИЙОМІ
        MOV   SP,#72H             ;
        CLR   P3.4          ; СКИДАННЯ СИГНАЛУ КЕРУВАННЯ АЦП
        CLR   P3.5          ;
        SETB  TR1           ;ПУСК Т\Л1
        SETB  TR0           ;ПУСК Т\Л0
        SETB  EA            ; ДОЗВІЛ ПЕРЕРИВАНЬ
SH:  MOV   A,14H            ; ПЕРЕВІРКА ПРАПОРА "ШИФРУВАННЯ"
        JZ    DE            ; ПЕРЕХІД НА АДРЕСУ ЯКЩО A=1
        MOV   00H,#38H      ;ВСТ.ПОЧ.АДРЕСИ ДАНИХ ДЛЯ ШИФРУВАННЯ
        MOV   01H,#30H      ;ВСТ.ПОЧ.АДРЕСА ДАННИХ ПОСЛЕ ШИФРОВАНИЯ
        JB    P3.2,SS             ; ВИЗНАЧАЄМО РЕЖИМ РОБОТИ
        MOV   A,15H         ; ПЕРЕВІРКА НА ПАУЗУ В МОВІ
        JNZ   SHIFR         ; ПЕРЕНОС 8-МИ БАЙТ У БУФЕР ПЕРЕДАЧІ БЕЗ ШИФРУВ
SS:     CLR   RS1           ; ВИБІР БАНКУ 0(1)
        CLR   RS0           ;
        MOV   R7,#8         ; ПЕРЕНОС З @R0 В @R1
P_S:    MOV   A,@R0;--\\--
        MOV   @R1,A         ;--\\--
        INC   R0            ;--\\--
        INC   R1            ;--\\--
        DJNZ  R7,P_S;--\\--
RE_SH:        MOV   00H,#38H    ; ПОВЕРНЕННЯ ПІСЛЯ ШИФРУВАННЯ
        MOV   01H,#30H      ; И ВТАНОВЛЕННЯ ПОЧЮ АДРЕС
        MOV   14H,#0        ; СКИДАННЯ ПРАПОРА ШИФРУВАННЯ
        MOV   15H,#8        ; ПРАПОР "ПАУЗА В МОВІ"=НАЧ.ЗНАЧЕННЯ
DE:     MOV   A,13H         ; ПЕРЕВІРКА ПРАПОРА "ДЕШИФРУВАННЯ"
        JZ    KON           ;
        MOV   11H,#20H      ;ВСТ. ПОЧ.АДРЕС
        MOV   10H,#28H      ;--\\--
        JB    P3.2,DD       ; ПЕРЕХІД НА ДЕШИФРУВАННЯ
        MOV   A,16H         ; ПЕРЕВІРКА НА ПАУЗУ В МОВІ(НА ПРИЙОМІ)
        JNZ   DESHIFR       ; ПЕРЕХІД НА ПІДПРОГРАМУ ДЕШИФРУВАННЯ
        ; ПЕРЕНЕСЕННЯ 8-МИ БАЙТ ІЗ БУФЕРА ПРИЙОМУ ДО P1
```

```
DD:     SETB  RS1           ;ВИБІР БАНКУ 2
        CLR   RS0           ;---\\---
        MOV   R7,#8         ;
P_S1:   MOV   A,@R1;ПЕРЕНОС ИЗ @R1 В @R0
        MOV   @R0,A;--\\--
        INC   R0            ;--\\--
        INC   R1            ;--\\--
        DJNZ  R7,P_S1       ;--\\--
RE_DE:        MOV   11H,#20H    ;УСТ.НАЧ.АДРЕСОВ
        MOV   10H,#28H      ;--\\--
        MOV   16H,#8        ; СКИДАННЯ ПРАПОРА "ПАУЗА В МОВІ НА ПРИЙОМІ"
        MOV   13H,#0        ; СКИДАННЯ ПРАПОРА "ДЕШИФРУВАННЯ"
KON:    MOV   A,12H         ; ПЕРЕВІРКА ЛІЧИЛЬНИКА ПРИЙОМУ
        JNZ   SH1           ;
        SETB  P3.6          ;ВКЛ.СВІТЛОДІОДУ
        AJMP  SH            ;
SH1:    CLR   P3.6          ;ВИМК. СВІТЛОДІОДУ
        AJMP  SH            ;
SHIFR:  CLR   RS1           ; ПІДПРОГРАМА ШИФРУВАННЯ (УМОВНО)
        CLR   RS0         ;
        MOV   R7,#8       ;
        MOV   R0,#30H     ;
SHY:    MOV   A,R7        ;
        MOV   @R0,A;
        INC   R0          ;
        DJNZ  R7,SHY      ;
        AJMP  RE_SH ;ВИХІД ИЗ П\П
DESHIFR:SETB      RS1   ; ПІДПРОГРАМА  ДЕШИФРУВАННЯ
        CLR   RS0   ;
        MOV   R0,#28H     ;
        MOV   R7,#8 ;
DF:     MOV   A,R7  ;
        MOV   @R0,A
        INC   R0
        DJNZ  R7,DF ;
```

```
        AJMP  RE_DE


; ОБРОБКА ПЕРЕРИВАНЬ ВІД INT0(НАТИСНУТА КНОПКА ЗАКРИТА ПЕРЕДАЧА)INTER0:
        PUSH  PSW           ;ЗБЕРЕЖЕННЯ PSW
        SETB  RS1           ;ВСТ.БАНКУ 3
        SETB  RS0           ;--\\---\\--
        MOV   R3,A          ;ЗБЕРЕЖЕННЯ АК.
POTER:  MOV   R2,12H                ;
        CJNE  R2,#0,NO      ; ПЕРЕВІРКА НА УТРАТУ ВХІДНОГО СИГНАЛУ
        CLR   P3.6          ; ГАСІННЯ СВІТЛОДІОДУ
        MOV   R5,#0FH       ; ЗАТРИМКА
TIM2:   MOV   R4,#01H       ; ЗАТРИМКА
TIM1:   MOV   A,R4          ;
        DJNZ  R4,TIM1       ;
        DJNZ  R5,TIM2       ;
        SETB  P3.6          ;ВКЛ. СВІТЛОДІОДУ
        MOV   R5,#0FH       ; ЗАТРИМКА
TIM4:   MOV   R4,#01H       ;
TIM3:   MOV   A,R4          ;
        DJNZ  R4,TIM3       ;
        DJNZ  R5,TIM4       ;
        AJMP  POTER         ;
NO:     MOV   R0,#40H       ;ВСТ.ПОЧ. АДРЕСИ КЛЮЧА В ЗУПД
        MOV   R1,#0         ;---\\---\\---\\---\\--- ВПЗУ
        MOV   R4,#8         ;КІЛЬКІСТЬ БАЙТ КЛЮЧА
KEY:    MOVX A,@R1;ЗЧИТУВАННЯ В ПЗП
        MOV   @R0,A;ЗАПИС КЛЮЧА В ЗУПД
        INC   R1            ;
        INC   R0            ;
        DJNZ  R4,KEY        ;
        MOV   A,R3          ; ВІДНОВЛЕННЯ АК.
        POP   PSW           ; ВІДНОВЛЕННЯ      PSW
        RETI                ; ВИХІД З ПІДПРОГРАМИ.
```

```
; ПІДПРОГРАМА ОБРОБКИ ПЕРЕРИВАНЬ ВІД INT1(НАТИСНУТА КНОПКА ВВЕДЕННЯ КЛЮЧА)
INTER1: PUSH    PSW   ;ЗБЕРЕЖЕННЯ PSW
        SETB    RS1   ;БАНК 3
        SETB    RS0   ;
        MOV     R3,A  ;ЗБЕР.АКК
        MOV     R0,#40H       ;ВСТ ПОЧ АДРЕСИ КЛЮЧА В ЗУПД
        MOV     R1,#0 ;---\\---\\---\\--- В ВПЗУ
        MOV     R4,#8 ;
KEY2:   MOVX    A,@R1;
        MOV     @R0,A;
        INC     R1    ;
        INC     R0    ;
        DJNZ    R4,KEY2       ;
        MOV     A,R3  ;
        POP     PSW   ;
        RETI          ;?
; ПОДПРОГРАММА ОБРАБОТКИ ПРЕРИВАНИЙ ОТ УАПП
SER_P:  JBC     RI,PR  ; ІДЕНТИФІКАЦІЯ ДЖЕРЕЛА
        JBC     TI,ENDP       ;
        AJMP    ENDP  ;
PR:     PUSH    PSW   ;
        SETB    RS1   ;ВИБІР БАНКУ 2
        CLR     RS0   ;--\\--
        MOV     R7,A  ;ЗБЕР.АК
        MOV     12H,#3; ВСТАНОВЛЕННЯ ЛІЧИЛЬНИКА ПРИЙОМУ
        MOV     P1,@R0; ПЕРЕДАЧА В P1 ДЕШИФРОВАННОЙ ИНФОРМАЦИИ
        SETB    P3.5  ; ФОРМУВАННЯ СИГНАЛУ ЗЧИТУВАННЯ ДЛЯ ЦАП
        INC     R0    ;
        CLR     P3.5  ;
        CJNE    R0,#30H,IN_1          ; СТЕЖИМО ЩОБ ЧИСЛО НЕБУЛО БІЛЬШЕ 2FH
        DEC     R0
IN_1:   JNB     RB8,IN4       ;
        MOV     R1,#20H       ; ВСТ ПОЧ АДРЕСИ (ДАНІ ДЛЯ ДЕШ)
        AJMP    INF
```

```
IN4:    CJNE   R1,#27H,INF
        MOV    13H,#1          ; ВСТАНОВЛЕННЯ ПРАПОРА "ДЕШИФРУВАННЯ"
INF:    MOV    A,SBUF          ; ЗЧИТУВАННЯ БУФЕРА ПРИЙОМУ
        MOV    @R1,A;
        JNZ    IN2     ;   ПЕРЕВІРЯЄМО ЧИ НЕ ДОРІВНЮЄ ПРИЙНЯТИЙ БАЙТ НУЛЮ
        DEC    16H     ;ПРИ 16H=0 - ПРАПОР "ПАУЗА В МОВІ"
IN2:   INC     R1      ;
IN3:    CLR    P3.6    ; ГАСІННЯ СВІТЛОДІОДУ
        MOV    A,R7    ; ВІДНОВЛЕННЯ АК
POP     PSW    ;
ENDP: RETI             ; ВИХІД З ПІДПРОГРАМИ.

; ПІДПРОГРАМА ОБРОБКИ ПЕРЕРИВАНЬ ВІД Т\Л0
TIMER:          PUSH  PSW    ;
        SETB   P3.4    ; ФОРМУВАННЯ СИГНАЛУ ДЛЯ УПР. АЦП
        CLR    RS1     ;ВИБІР БАНКУ 0(1)
        CLR    RS0     ;---\\---
        MOV    R3,A    ;ЗБЕР. АК
        CLR    P3.4    ;
        MOV    A,12H   ;
        JZ     TC      ;
        DEC    12H     ; ЛІЧИЛЬНИК ПРИЙОМУ
TC:     MOV    A,P2    ; ЗЧИТУВАННЯ Р2
        MOV    @R0,A;И ЗАПИСЬ В ЗУПД
        JNZ    M       ;
        DEC    15H     ;15H=0- ПРАПОР "ПАУЗА В МОВІ"
M:      CJNE   R0,#3FH,NET;В R0 АДРЕСА 8-ГО БАЙТА
        MOV    R0,#38H         ; ВСТ.ПОЧ.АДРЕСИ ДАНИХ ДЛЯ ШИФРУВАННЯ
        MOV    14H,#1          ; ВСТАНОВЛЕННЯ ПРАПОРА ШИФРУВАННЯ
        AJMP   NET0  ;
NET:    INC    R0      ;
NET0:    MOV   A,12H ; ПЕРЕВІРКА ПРАПОРА 'ВТРАТА ВХ.СИГНАЛУ'
        JNZ    PER     ; ПЕРЕХІД НА АДРЕСУ ЯКЩО АК НЕ =0
        MOV    @R1,#0          ; СТИРАЄМО БАЙТ
PER:    CJNE   R1,#30H,N     ;В R1 АДРЕСУ 1-ГО БАЙТА?
```

```
        SETB  TB8    ;
        AJMP  PE1    ;
N:    CLR     TB8    ;
PE1:  MOV   SBUF,@R1     ;ПЕРЕДАЧА В УАПП
        INC     R1       ;
        CJNE   R1,#38H,PE2 ;ЯКЩО В R1 38H ТО СКИДАННЯ R1
        MOV   R1,#30H       ;
PE2:  MOV   A,R3   ;
        POP    PSW   ;
        RETI   ;
        END
```

Додаток 2. Перелік елементів

Поз. Позн.	Найменування	**Кіл.**	**Примітка**
Q1	Кварцовий резонатор 55 МГЦ	1	
S2	Кнопка П-2К	1	
C4	Конденсатор К50-12-10 мкФ±10%	1	
C1	Конденсатор КМК-2А-100 пФ±10%	1	
C2,C3	Конденсатор КМК-2А-30 пФ±10%	2	
DD4	Мікропроцесор DS87C520	1	
DD2	Мікросхема AD557	1	
DD1	Мікросхема AD7574	1	
DD6	Мікросхема M27C256B	1	
DA1,DA2	Мікросхема К140УД20А	2	
DD3	Мікросхема SN74LS05	1	
DD5	Мікросхема DM74ALS573B	1	
S3	Перемикач DIP-7	1	
S1	Перемикач П-2К-1	1	
R1,R2,R4,R5	Резистор МЛТ-0,125-301 Ом ±5%	4	
R3,R6-R14	Резистор МЛТ-0,125-10 кОм ±5%	9	
R15	Резистор МЛТ-0,125-100 кОм ±5%	1	
R18-R27	Резистор МЛТ-0,125-3 кОм ±5%	10	
R17	Резистор МЛТ-0,125-8,2 Ом ±5%	1	
VD1	Світлодіод АЛ307Л	1	